Brussels, April 27th, 2020

THE EUROPEAN DATA PROTECTION SUPERVISOR's ANSWERS TO THE QUESTIONS ISSUED BY THE COMMITTEE FOR EUROPEAN AFFAIRS OF THE SENATE OF THE REPUBLIC OF FRANCE

- **Q1: How is cooperation organized with and between national data protection authorities during the current crisis? How did you adapt your working methods and exchanges?**

Under normal circumstances, The European Data Protection Board (EDPB) – the body consisting of all data protection Supervisory Authorities of EU and EEA states as well as EDPS - meets on average once per month, in-person, on Plenary sessions in Brussels, while each of the seven Expert Groups meets also once a month. Due to the current crisis, we quickly **switched to remote meetings via video- and teleconference**. This now applies both to the internal Expert Groups, as well as the Plenary meetings which brings together the heads of supervisory authorities. While Expert Groups meet virtually more or less according to previous schedule, the **frequency of the EDPB plenary meetings has increased considerably** during the past few weeks in light of the urgent need for guidance on matters related to the COVID19 outbreak, and the virtual plenary was organised twice a week on Tuesdays and Fridays. Most recently the EDPB adopted Guidelines on the processing of health data for scientific research purposes, as well as on the use of location data and contact tracing tools in the context of the

COVID-19 pandemic. In the absence of physical meetings, we also increasingly make use of **written procedures** as a means to adopt our opinions and guidance.

- **Q2: Would you please remind us which European regulation (GDPR, e-privacy, etc) is relevant to the debate on contact tracing applications? Could the regulation (EU) 2018 2018/1725 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies be pertinent, in case of a deeper involvement of the EU?**

a) General legal framework:

As **contact tracing applications are** currently being considered in individual Member States, their deployment is **primarily governed by the General Data Protection Regulation** (GDPR) and the **ePrivacy Directive** and its implementing national legislation.

The General Data Protection Regulation in principle applies to the processing of personal data by private and public entities throughout the EU. The so-called the ePrivacy Directive applies to the processing of personal data in the context of electronic communications networks. It also contains specific rules in case of storage of information (or access to information already stored on) an end-users device, which is the case for contact tracing applications. Though GDPR exists in the form of Regulation which is therefore directly applicable, binding and effective in all Member States it has to be complemented by national law (e.g., procedures). Member states also enjoy some flexibility (room for manoeuvre) in certain specified areas, where they can notify the European Commission that they chose to use the legal solution which differs from the line proposed in GDPR, to make the choice offered by GDPR. Some provisions done under first group may play a role for Covid-19 tracing apps as health services are mainly regulated by national law and medical data under national law may enjoy further reaching protection in national law than data concerning health enjoys under GDPR. An example of room for manoeuvre offered by GDPR which may have an influence on construction of an app we comment is the determination of the age of consent for the minors (13-16 years).

Regulation (EU) 2018/1725

Regulation (EU) 2018/1725 **(**EUI GDPR**)** applies to the processing of personal data by (and among) European Union institutions, offices, bodies and agencies, and replicates the provisions of the GDPR. It would play a central role if a contact tracing app was developed by an EU

institution (EUI). However **I am currently not aware of any plans** for the EU institutions to introduce a contact tracing application of their own.

Decision No 1082/2013/EU (EWRS Decision)

Nevertheless, Decision No 1082/2013/EU on serious cross-border threats to health establishes a system for the coordination and exchange of personal data between Member States involved in contact-tracing measures.

It provides for an **Early Warning Response System (EWRS**), which links the European Commission, European Centre for Disease Prevention and Control (ECDC) and public health authorities in the EU and EEA countries responsible at national level for notifying alerts related to serious cross-border threats to health. Such **notifications may include personal data necessary for the purpose of contact tracing**.

The main aim of EWRS is to ensure that competent public health authorities in Member States and the Commission are duly informed in a timely manner. It enables the Commission and the competent authorities responsible at national level to be in permanent communication for the purposes of alerting, assessing public health risks and determining the measures that may be required to protect public health.

In relation to their responsibilities to notify personal data through the EWRS, the national competent authorities act as controllers, i.e. are responsible under data protection law. However, in relation to its **responsibilities concerning storage of personal data, it is the European Commission that acts as a controller**. Both the GDPR and Regulation (EU) 2018/1725 are applicable to this processing of personal data.

- **Q3: What is your opinion on the guidance and the toolbox issued par the European Commission? Were you consulted? Is your view different? On which matters?**

I welcome the European Commission's Recommendation, Guidance and Toolbox for Member States on the use of mobile applications to support contact tracing.

As the virus knows no borders, the need to ensure a pan-European approach is clear. As a matter of fact, it was the EDPS who first publicly called for such a pan-European approach in relation to contact tracing applications.

I am very pleased to see that the Commission guidance echoes our position and that of the EDPB in many respects, including:

- the need for pan-European approach;
- the recognition that data and technology may be part of the solution, it is only one element, and by no means a "silver bullet";
- the importance of using data and technology as a tool to empower, rather than control, stigmatise or repress individuals;
- the need to ensure that measures deployed in times of crisis are temporary by nature.

The European Commission formally consulted the European Data Protection Board on its draft Guidance document. Earlier on, the EDPS also advised the Commission on the possibility to use aggregated and anonymised location data.

- **Q4: As far as you know, is the implementation of such applications generally based on objective and transparent assessment of the expected health benefit (how efficient these apps could be in stemming the epidemic)? Would you recommend a check of the effectiveness of the device from this point of view after a while? When?**

The potential effectiveness of contact tracing applications (or lack thereof) is of fundamental importance. While there is great pressure on policymakers to act, not every use of data or technology is in fact going to help us fight the pandemic in a meaningful way.

We are aware of the complete failure of mobile apps in monitoring the spread of Ebola virus in 2016, as well as very poor results of the use of apps to help the authorities to fight two other pathogens in Kenya. We are also aware of the estimations of specialists who state that the apps may be an important tool to fight with the spread of Coronavirus if they are **used** by approximately 60 % of population and that apps would be completely useless if they are not used by at least 20 % of population. Bearing in mind that relatively highly "tech-skilled" and well organised Singaporean society reached initially the level of 12% population using *TraceTogether* app (improving to ca. 20 % today) we are of the opinion that it will be extremely hard to reach expected proliferation of app amongst Europeans. Nevertheless it might be possible and it is worth to try while it is done with proper safeguards and without overreaching expectations as far as effectiveness is concerned.

We must also recognise that the effectiveness of a specific measure will depend primarily on factors outside data protection law, such as the spread of the virus at that moment in time as well as traditional tracing and testing capabilities, as well as the overall exit strategy deployed in a particular Member State.

It is essential that governments, in consultation with the relevant experts from epidemiology and virology, develop solutions based on a transparent assessment of the perceived efficiency of contact tracing applications. Transparency is particularly important in order to enable the public trust is essential for the successful implementation of such applications.

As it was mentioned above, my personal position is that it is worth trying to develop effective contact tracing apps as long as specialists (epidemiologists and public health officials in particular) say that they are useful and necessary. At the same time we have to remember that apps will not be "silver bullets" and they will not solve the problem alone. They need first of all to be based on solid health services, availability of tests, continued manual tracing and proper

sociological and psychological support for those who are "informed" "by app" on the "probability of being infected" especially in the case of so called false positive cases.

If that turns out that the effectiveness of apps is too low, such applications should be dismantled, as otherwise they may negative effects, such as promoting a false sense of security or remove the focus from other measures which are more effective. The worst scenario would be if we try to fight against the effectiveness of the applications being lower than expected by adding new – not tested enough – functionalities. The extreme example of such functionality is so called "immunity passport" or "green code" based on assumptions not confirmed by medicine and automatically generated by some apps used outside of EU.

I therefore **agree with the CNIL's opinion** issued last weekend that it is important to periodically review the approach that is taken. If the evidence shows that a particular is not or no longer fit for purpose, it needs to be reconsidered.

- **Q5: The more people use the application, the more efficient it is, according to epidemiologists. So how important is the issue of interoperability with regard to the proportionality of the intrusiveness of those apps?**

As it was written in the answer to Question 4) the potential effectiveness of contact tracing applications (or lack thereof) is of fundamental importance. While there is great pressure on policymakers to act, not every use of data or technology is in fact going to help us fight the pandemic in a meaningful way.

We are aware of complete failure of mobile apps in monitoring the spread of Ebola virus in 2016, as well as very poor results of the use of apps to help the authorities to fight two other pathogens in Kenya. We are also aware the estimations of specialists who state that the apps may be an important tool to fight with the spread of Coronavirus if they are **used** by approximately 60 % of population and that apps would be completely useless if they are not used by at least 20 % of population. Bearing in mind that relatively highly "tech-skilled" and well organised Singaporean society reached initially the level of 12% population using *TraceTogether* app (improving to ca. 20 % today) we are of the opinion that it will be extremely hard to reach expected proliferation of app amongst Europeans. Nevertheless it might be

possible and it is worth to try while it is done with proper safeguards and without overreaching expectations as far as effectiveness is concerned.

Interoperability is essential. Any exit strategy that will provide more freedom to people's movements and remove travel restrictions must take into account that people will cross national borders.

So it has to be designed in a way to be able to operate and interact with different but similar applications. This is crucial to continue providing the same results on contact tracing for the benefit of all individuals and public health.

We know from experts from the European Centre for Disease Control (ECDC) that traditional, manual approaches to contact tracing are very difficult if not impossible to implement in case of cross-border travel, which obviously is very common in Europe. Contact tracing apps can help solve this difficulty, but only on the condition that the national approaches are coordinated and (at least) interoperable.

This is why we strongly welcome the European Commission's efforts to development of pan-European approach in relation to contact tracing applications.

Interoperability is required on many different levels: technological, semantic, organisational and legal (see the European Interoperability Strategy 2010 and the European Interoperability Framework 2017). That includes functional requirements, technical specifications, epidemiological frameworks and security. But we also need to ensure that there are the right safeguards for personal data protection built in from the start, so that every citizen in every Member State can have confidence that the use of such an application does not undermine his fundamental rights and freedoms, which the EU and the EU treaties are meant to protect.

All solutions, interoperable or otherwise, should be proportionate. This means that least intrusive solutions should always be preferred, taking into account the specific purpose pursued by the measure in question.

- **Q6: About 300 researchers expressed their concern about the centralized architecture of the PEPP-PT initiative. But in France, the chairman of the research organization INRIA explained that a peer-to-peer solution couldn't be used for such applications, due to security vulnerability. Could you explain us the differences between centralized and decentralized applications, and the pros and the cons of each solution?**

As EDPS we keep a close eye on PEPP-PT and other relevant initiatives, including the DP-3T project. We have been first informed on the possibilities of *Bluetooth* technologies in contact tracing already on March 27th, and we have been explained what might be a difference between so called centralised and decentralise approach on April 6th by scientists themselves (especially by Prof. Bart Preneel from the Catholic University of Leuven – co-operating with DP-3T). I have been also taking part in webinars both with representatives of PEPP-PT (Hans-Christian Boos – Arago GmbH) and DP-3T (its leader Prof. Carmela Troncoso - EPFL Lusanne and Dr. Michael Veale - University College London).

Centralised and decentralised approaches are currently heavily debated. While the debate is strongly polarised, it is by no means a binary proposition. Even under the decentralised approach, there will be some forms of processing activities that take place centrally in order for the system to function. Likewise, the so-called centralised model involves processing which is local.

Similarly, some form of a central server is always needed. The main question is therefore: what is centralised and why. What is most important is whether a particular approach is fit for purpose, so that it can support efficiently the epidemiological tracking of infections.

Depending on the particular design, the risk model of data confidentiality and identification changes. Any potential technical solution will need to justify its risks and countermeasures. A properly executed data protection impact assessment should precede the decision: Which privacy risks do we want to consider particularly important? What amount of trust in the central server do we want to accept?

[*In more detail: the main distinguishing features are:*

- *How the ephemeral identifiers of the user devices that are broadcast with Bluetooth LE are generated*

  In some centralised settings, this ID is generated centrally and liaised by the server. This allows the authority who manages the server to control this ID and it creates

certain risks. In our view, the ID could and should always be generated on device, irrespectively if the overall setting of the system is centralised or not.

- *If in a centralised setting the server requires the application sends information about all the encountered devices (their IDs), it can also be used to create a local or global proximity maps between contacts (a type of social graph). This creates concern as it would potentially allow the monitoring of movement and contacts between all the users in the system.]*

So we need to be clear why some things are done centrally and why some things are done locally and what the associated risks are. We need to think about this not only from a security perspective, but also from the perspective minimising the risk of re-identification and undesirable re-use in the future.

The Opinion which was issued last weekend the CNIL identifies a number of important safeguards which should be put in place, e.g. to prevent risks of re-identification.

Because once the infrastructure is in place, it may be very tempting to use the data collected for additional purposes which are currently not being considered ("function creep").

The EDPB guidance actually lists data protection considerations and safeguards for both centralised and decentralised approaches.

- **Q7: Do you recommend a decentralized data storage model? Would it limit the effectiveness of the apps?**

[See response to Q6 for an introduction]

While the degree of (de)centralisation is an important factor to consider from a data protection perspective, it is by no means a binary proposition. Everything depends on the specific use case (what exactly do we want to achieve) and safeguards applied.

As far as effectiveness is concerned, it is also not simply a matter of centralisation or decentralisation. Some public health purposes can be achieved effectively and efficiently under a decentralised approach. At the same time, there may be a trade-off between deploying a fully decentralised approach and the kind of information that would be made available to public health authorities through these applications.

We also always need to consider: do we need the same application or server to perform every useful activity?

Contact tracing applications, if deployed, must be part of a broader set of measures (e.g., testing, manual contact tracing) which each have their own procedures, data collection and storage associated with it. So not every purpose needs to be achieved via the contact tracing applications alone.

We need to think carefully about which functionalities to introduce in the same application, also with a view of minimising the risk of function creep in the future.

- **Q8: Do all European countries chose to rely on tracing (or tracking) apps? At which stage of the epidemics?**

Not all European countries have chosen to rely on contact tracing or tracking apps.

While in some countries contact tracing or tracking applications have already been deployed; other countries are still considering deployment and are various stages of technical development.

At EU level, contact tracing apps are being considered primarily as part of exit strategy. The use of such mobile applications are considered particularly relevant in the phase of lifting containment measures, when the infection risk grows as more and more people get in contact with each other.

The right moment of deployment may vary from Member State to Member State, depending on the general exit strategy and also taking into account the testing capabilities and capacity of the healthcare system.

- **Q9: Which technical solutions are used or planned to be used for now? Is users anonymity guaranteed? Which authorities are responsible for data processing? Can third parties (in particular private firms) be implied?**

As far as contact tracing is concerned, many experts propose use of Bluetooth LE (Low Energy) for proximity detection and for the data exchange mechanism that alert participants of possible exposure.

Bluetooth Low Energy (BLE) communications between devices appears more precise, and therefore more appropriate, than for example the use of geolocation data (GNSS/GPS, or cellular location data), which would likely not work indoor, sometimes even outdoor, due to the limited precision. So in my view Bluetooth is an appropriate solution.

Furthermore, BLE can be used in such a way as to reduce tracking (contrary to the use of raw geolocation data). The European Commission therefore also recommends the use of BLE communications data (or data generated by equivalent technology) to determine proximity.

The EDPB and CNIL have also confirmed that information on the proximity between users of the application can be obtained without locating them. This kind of application does not need, and, hence, should not involve the use of location data. Moreover, there are doubts that other techniques could be equally precise.

Contact tracing application are intended to help notify individuals of the fact that they have been in close proximity of someone who is eventually confirmed to be a carrier of the virus, in order to break the contamination chains as early as possible. This does not require direct identification of the users and all appropriate measures should be deployed exclude or minimise the risks of re-identification. The Opinion of the CNIL issued this weekend identifies a number of important safeguards in this regard.

While the risk of re-identification can be minimised, in particular under a decentralised approach, I would not say that users are anonymous. Ultimately, the purpose of these applications is to influence the behaviour of specific individuals. Moreover, with additional data and enough resources, it may be possible to re-identify individuals. But assuming that we need applications for contact tracing, we should ensure these applications are well designed to minimize privacy risks.

Different authorities and bodies are involved in the deployment of contact tracing applications. The designation of public health authorities as the responsible entity is consistent with the approach that contact tracing apps should be deployed as public health tools which are provided in order to further empower citizens, rather than to control, stigmatise or repress individuals.

However, other entities can also controllers and therefore responsible under data protection law. For example, in AT, it is the Red Cross which developed and made available a contact tracing application.

Governments can make use of the services offered by private actors when developing and deploying contact tracing applications. Such service providers must be trustworthy however, which means that they must provide sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of the GDPR.

Moreover, a binding legal arrangement must be put in place to ensure that any personal data is processed exclusively on the instructions of the controller and to ensure a continuous level of protection.

- **Q10: Do you consider that the technical solutions proposed by French and German researchers ("Robert" protocol") are compliant with European rules?**

The currently available information indicates that the ROBust and privacy-presERving proximity Tracing scheme (so called Robert protocol) is based on the principles of voluntary use, transparency, preservation of anonymity and interoperability. Its goal is to preserve data privacy and retain also its security.

It seems to be a centralised scheme where it is guaranteed that the central authority should not be able to learn the identities or locations of the users. However, as we do not know how exactly the solutions using Robert protocol would process the data on the server at this point, answering this question without full details is unfortunately not possible today.

- **Q11: Do you think the use of such apps should or could be compulsory? On which legal basis (already existing, newly introduced through the legal response to the health crisis)? Could you explain why the voluntary use of such apps does not mean that the processing of personal data will necessarily be based on consent?**

I agree with my EDPB colleagues that the use of such applications should be voluntary.

I also consider that the mere fact that the use of contact-tracing applications takes place on a voluntary basis does not mean that the processing of personal data by public health authorities will necessarily be based on consent.

When public authorities provide a service based on a mandate assigned by and in line with requirements laid down in law, the most relevant legal basis for the processing is the necessity for the performance of a task in the public interest. The CNIL also confirmed this in its recent Opinion concerning the StopCovid app.

Contact tracing applications are being considered as part of the general response of those public authorities to the current crisis. The actions taken by those public authorities are undeniably part of the task of public interest with which they have been entrusted.

In any event, the deployment of contact tracing applications should be accompanied by a clear legal framework, which clearly sets out certain limits and provides for meaningful safeguards (such as a clear purpose specification and explicit limitations on further use, identification of who will have access to the data and for which purpose, etc.).

Reliance on a consent-based approach alone is simply not tenable from the perspective of the principle of legality that must underpin the actions of public authorities.

Whether or not a new legislative measures need to be adopted or whether it is possible to rely on an existing legal basis depends on the laws already in place in each Member State. It also depends on the degree of interference: the more serious the interference, the greater the need for detailed safeguards to be included in the law.

- **Q12: Regarding data retention, the data should be erased after the epidemic. Under which conditions could these data be kept for research purposes?**

Article 89 of the GDPR provides the general conditions for the processing of personal data for scientific research purposes. It stipulates that the processing of data for research purposes "shall be subject to appropriate safeguards" and that those "safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation."

In scientific research, data minimisation can be achieved through the requirement of specifying the research questions and assessing the type and amount of data necessary to properly answer these research questions.

If it is possible to perform the scientific research with anonymised data, the data should be anonymised as soon as possible and not kept in a form which allows the identification of the data subjection for longer than is necessary. The CNIL also confirmed this in its recent Opinion concerning the StopCovid app.

Where anonymisation is not possible, pseudonymisation should be considered.

In any event, the data is needed depends on the specific purpose of the research in question. Even when the research has an explorative nature, it should always comply with the purpose limitation principle.

In order to define storage periods (timelines), criteria such as the length and the purpose of the research should be taken into account.

It has to be noted that national provisions may stipulate rules concerning the storage period as well.

Finally, I wish stress that we need to carefully consider which data and which data sources we want to use for research purposes. Relevant data may be collected at different stages of the process, and it is essential that we use the right data sets so we can draw the right conclusion afterwards.

- **Q13: In France, Parliament debate on 28 and 29 April on a draft version of the tracing app that could be rolled out, not on the final version. Do you know if such a debate is taking place in all Member States?**

I am not able to say whether every parliament in every Member State is debating the use of contact tracing apps. Not all Member States are considering the use of contact tracing applications to the same extent.

Where contact tracing applications are being considered, however, I firmly believe that they should be the topic of democratic debate. In the Netherlands, for example, such debates are already taking place and in Belgium members of parliament have recently introduce a resolution to call for a parliamentary debate.

- **Q14: Will the EDPS formulate an opinion on the final version of every national application?**

No. As advisor to EU institutions, it is not role of EDPS to formally assess the compliance of contact tracing applications adopted at national level.

I am also not aware of any plans yet to do this at the EDPB level. The EDPB has already issued specific guidance that should be used to inform the development and subsequent assessment at national level, to ensure GDPR compliance.

It will in principle be a matter for each national supervisory authority to decide whether to make such an assessment (e.g. in the context of a complaint or own-initiative investigation)

- **Q15: If the applications based on Bluetooth technology were not efficient enough (let's say due to technical issues), would you consider the use of geo-tracking? Under what conditions?**

[See also answer to the Question 9)]

As far as contact tracing is concerned, the use of Bluetooth LE (Low Energy) is recommended as it appears to be more precise, and therefore more appropriate, than the use of geolocation data (GNSS/GPS, or cellular location data). Moreover, BLE avoids the possibility of tracking (contrary to geolocation data).

As long as it possible to obtain useful information on the proximity between users of the application without locating them, geo-tracking should not be used. The purpose of contact tracing application in principle does not need, and, hence, should not involve the use of location data.

We should note that the geo-tracking of specific individuals for public health purposes would represent a far greater intrusion into the private lives of individuals.

Geo-tracking should therefore not even be considered as long as not necessary to achieve the purpose in a reasonably efficient and effective manner.

- **Q16: Some Member States also developed applications aimed at checking compliance with quarantine obligations. Should those applications be considered as in breach with the European regulation?**

I firmly believe that data and technology should be used to empower, rather than to control, stigmatise, or repress individuals.

We are at a very delicate stage in history. The ability of citizens to trust their governments is essential in times of crisis. Using applications to enforce quarantine essentially starts from the presumption that the individual cannot be trusted to act responsibly. Can governments expect citizens to trust them if citizens are automatically distrusted by their governments?

From a legal perspective, any use of location data or applications to enforce quarantine would require the adoption of a specific legislative measure. However, such exceptional legislation is only possible if it constitutes a necessary, appropriate and proportionate measure within a democratic society.

I have my doubts whether would be possible to demonstrate the necessity and proportionality of such applications, given the grave interference it would represent. We would be talking combined use of use of location data and health data in order to restrict and automatically monitor the movement of individuals. This would be a game changer from a data protection and privacy perspective and could have long-lasting effects on the balance of power between citizens and governments, also after the crisis has passed.

- **Q17: Were specific measures adopted regarding data protection, to support the wider use of telemedicine during the epidemic?**

I am not aware of any specific measures regarding data protection being adopted to support the wider use of telemedicine during the epidemic.

The use of mobile application to help the diagnosis or allow doctors to provide advice to patients has been considered as part of the Commission's recommendation and toolbox on the use of technology and data to combat and exit from the COVID-19 crisis.

When mobile applications are used for those purposes, they could be considered as medical devices and would therefore fall within scope of under Regulation (EU) 2017/745 of the European Parliament and of the Council or Council Directive 93/42/EEC.