Brussels, 27 April 2020

THE EUROPEAN DATA PROTECTION SUPERVISOR's

INTRODUCTORY REMARKS BEFORE

THE COMMITTEE FOR EUROPEAN AFFAIRS OF THE SENATE

OF THE REPUBLIC OF FRANCE

Honorable President Bizet,

Ladies and Gentlemen,

Thank you for inviting me.

The debate you are having today is of historic importance.

Since the beginning of the COVID-19 pandemic, data and technology have been touted as indispensable to fight this existential threat to Europeans, to our economy and to our way of life.

Now, after extended periods of general confinement, officials are working hard on an exit strategy.

Important decisions are about to be made on the role of data and technology as part of that strategy. The choices made in the coming days will impact not only our immediate future, but resonate for years to come.

Before offering you my modest contribution, I want to clarify the role of the EDPS in this debate.

The European Data Protection Supervisor (or "EDPS") is the independent supervisory authority of EU institutions and bodies. We do not supervise the processing activities carried out by national governments. That is the role of national supervisory authority which in France is CNIL.

The European Data Protection Board (or EDPB) brings together the independent supervisory authorities of the European Economic Area, such as the CNIL, as well as the EDPS.

While we have the same acronym in French ("CEPD"), it is important to note that the EDPS and EDPB are in fact two different entities, with a different composition and competences.

What we share, however, is our common objective to ensure a high level of protection of natural persons with regard to the processing of personal data.

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.

I firmly believe that the digital revolution has given us powerful tools that, if used responsibly, can be of great help to governments who are trying to square the circle of protecting lives as we move to lift restrictions and gradually restart the European economy.

In my view, responsibility also means that we should not hesitate to act when it is necessary. There is also responsibility for not using the tools we have at our disposal to fight the pandemic.

As an EU body, it will not surprise you that the EDPS called for a pan-European approach to fight the pandemic. Together we are not only stronger, we can also be more effective.

I warmly welcomed the initiative undertaken by the European Commission to provide a toolkit for a pan-European approach. As EDPB, we have recently complemented the Commission's initiatives with our own guidance and recommendations. Just last Friday the CNIL issued its Opinion on the "StopCovid" mobile contact tracing application that is being considered in France.

All these contributions are tremendously valuable and important. Taking one step back, I believe that there are **three main considerations** that should inform how we want to use data and technology going forward.

1. Empowerment over control

First, I firmly believe that data and technology are most effective when used to empower, rather than to control, stigmatise, or repress individuals.

Trust in public authorities is essential in times of crisis.

If public authorities use technology to control the behaviour of individuals, it reveals a presumption that individuals cannot be trusted to act responsibly.

Can public authorities expect citizens to trust them if citizens are automatically distrusted?

2. There are no silver bullets

Second, while data and technology can be important tools, they are not a "silver bullet".

There is great pressure on policymakers to act. But not every use of technology is going to help us fight the pandemic in a meaningful way.

It is essential that governments, in close consultation with experts from epidemiology and virology, develop solutions based on a transparent assessment of their efficiency.

Many stakeholders are now questioning the effectiveness of contact tracing applications. My personal position is that we should consider the use of such applications as long as specialists (epidemiologists and public health officials in particular) say that they are useful and necessary.

If that turns out not (or no longer) to be the case, such applications should be dismantled. Otherwise they can have negative effects, such as promoting a false sense of security or forestall more basic and essential measures to manage public health.

But we must also be realistic: no technological support is going to work perfectly from day one.

That is why it is important to keep a long-term perspective: if governments now hasten to deploy intrusive measures or fail to put in place sufficient safeguards, irreparable damage will be done to the confidence in public authorities to manage the crisis responsibly.

3. Data protection is not the problem, it is part of the solution

Third, it should be clear to all stakeholders that data protection is not part of the problem, it is part of the solution.

Data protection imposes careful consideration of what we want to achieve, how we plan to achieve it and what impact to expect. These are good management practices, both for data processing and for public health.

Data protection also brings in transparency and accountability necessary for trustworthiness.

When it comes to contact tracing applications, a topic of some debate is whether to adopt a centralised or decentralised approach. While the debate is heavily polarised, 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.

From a data protection perspective, decentralisation is an important factor that can help to minimise risks for fundamental rights and freedoms and enhance user control.

But even under the decentralised approach, there will be a minimum of processing activities that take place centrally in order for the system to function.

So we need to be clear why some things are done centrally and why some things are done locally, what the associated benefits and risks are, and which measures can be put in place to address those risks.

I stated at the beginning of my intervention that the debate you are having today is of historic importance.

Only through close engagement among public health experts, technical developers and data protection authorities can we ensure that the solutions developed today will not have unintended consequences tomorrow.

I look forward to your questions.