22 October 2020

ENISA Annual Privacy Forum

Speech by European Data Protection Supervisor

Wojciech Wiewiórowski

Dear Juhan, Dear colleagues,
Ladies and Gentlemen,

I would like to first thank Juhan and ENISA for inviting me to join this event.

The EDPS has participated in the ENISA Annual Privacy Forum since its very first edition, and the cooperation between our organisations has developed and deepened over the years.

1. IPEN workshop

In the last few years, we have held our own **IPEN workshop** adjacent to this conference. IPEN is the Internet Privacy Engineering Network that the EDPS created after the Snowden revelations. ENISA has supported IPEN from the start.

We held an IPEN webinar yesterday focussing on the following question: *what can we learn in matters of data protection by design and **privacy engineering** from the experience of **COVID-19 contact tracing apps**?*

We heard from developers and data protection supervisory authorities, and there is indeed much to learn. The story of COVID-19 tracing apps is not over yet. The discussion about the apps, their value and limits has picked up speed, in view of the current development of the pandemic.

As privacy and cybersecurity are the focus of public debate, we will certainly have more exchanges on this topic.

I would like to thank those of you who have participated in the event yesterday. For those who could not make it, we will soon be making the materials and recordings available on our website.

2. Cooperation between ENISA and the EDPS.

Allow me to say a few more words about the **cooperation between ENISA and the EDPS.**

While ENISA and the EDPS each have their specific and very different roles and responsibilities at EU level, one could say that we are playing in the same field. This has become even more obvious this year as the European Commission has given digital policy a special focus in its work programme.

For the EDPS, it is a statutory responsibility to advise the EU legislators on the many initiatives which the Commission plans for its current mandate, wherever data protection or privacy are affected. ENISA will of course provide its expertise as well.

ENISA and the EDPS differ in many ways, organisational set-ups and mandates are very clear in this regard. We are taking our roles and tasks very seriously. We are the independent supervisory authority with regard to the processing of personal data by the Union institutions, bodies, offices and agencies. Therefore, ENISA is one of the agencies whose processing of personal data we oversee, and we are indeed doing this.

Nevertheless, our competencies and expertise are complementary, and we have common objectives to protect EU citizens against digital risks. Both ENISA and the EDPS work to ensure that EU citizens can exercise their fundamental rights and freedoms in the area of networks and electronic communications.

At the latest review of ENISA's regulation, the EDPS argued in its opinion that providing technical expertise on matters of privacy should remain on ENISA's list of tasks. Therefore, it is good to see that the Annual Privacy Forum continues to be a focal point for this cooperation.

While the EDPS has been developing its technological competence and capacity continuously, ENISA's expertise can still be a valuable complement to our own possibilities.

It is my intention **to take this cooperation with ENISA further** during this mandate, and my colleagues will cooperate with ENISA staff to make our already very good existing cooperation, even better.

3. Crossroads Of Technology And Privacy

The title of this panel is "crossroads of technology and privacy". When I look at the program of this event, there are a few keywords that appear several times:

Tracking

Tracing

Transparency

I think we can see these three terms as representatives of the challenges which data protection is facing today regarding the development of technology.

Tracing is becoming more and more pervasive. Citizens are at the risk of tracing with each transaction made on the Internet. With further digitalisation of our physical world, more of our actions can be traced. As an example, electronic means of payment connect more and more purchases to the identity of the user.

Transport is another area where tracing possibilities keep growing. Ride hailing services force users and drivers to use specific apps, which record all movements by time and location. Public transport providers use electronic means that record each travellers' interaction with the devices that provide access to the transport network. Some electric

car brands come equipped with "total surveillance as-a-feature" inside and outside their vehicles.

Mobile **communication** devices are the platform for many other tracing possibilities. Apart from the original service of electronic communications, they serve the purpose of recording other physical and virtual interactions. The COVID-19 tracing apps are illustrating only a small section of these possibilities.

In addition to tracing, **tracking** becomes ubiquitous, too. People can be observed by devices in the public sphere without their participation and knowledge. The recognition of car number plates has been used for an increasing number of purposes over the years.

Now we are entering a new phase of contactless tracking of individuals in public areas. **Remote facial recognition technology** has developed quickly; so much so that some authorities and private entities want to use it in many places. If this all becomes true, we could be tracked everywhere in the world.

I do not believe that such a development can be reconciled with the values and fundamental rights that are at the foundation of our democratic societies. The EDPS therefore, together with other authorities, supports a moratorium on the rollout of such technologies. The aim of this moratorium would be twofold. Firstly, an informed and democratic debate would take place. Secondly, the EU and Member States would put in place all the appropriate safeguards, including a comprehensive legal framework, to guarantee the proportionality of the respective technologies and systems in relation to their specific use.

As an example, any new regulatory framework for Artificial Intelligence (AI) should, in my view:

- apply both to EU Member States and to EU institutions, offices, bodies and agencies;
- be designed to protect individuals, communities and society as a whole, from <u>any</u> negative impact;

- propose a robust and nuanced risk classification scheme, ensuring that any significant potential harm posed by AI applications is matched with appropriate mitigating measures.

We must ensure that Europe's leading role in AI, or any other technology in development, does not come at the cost of our fundamental rights. Europe must remain true to its values and provide the grounds for innovation. We will only get it right if we ensure that technology serves both individuals and society.

Faced with these developments, **transparency** is a starting point for proper debate and assessment. Transparency for citizens puts them in a position to understand what they are subject to, and to decide whether they want to accept the infringements of their rights.

We have made progress regarding transparency with the full application of the GDPR. It is encouraging that the transparency mechanisms of the GDPR are being increasingly used to expose tracing and tracking mechanisms that have been introduced long ago without any public visibility - and therefore without public scrutiny.

Knowing about these mechanisms is the starting point to take actions against their excess. This can be statutory action by DPAs, but it can also be complaints by individuals or data protection associations and litigation in the courts. We are currently observing high profile cases in both domains and some recent court decisions from our highest court in the Union are encouraging us to think that the EU legal framework can show its full potential.

***

To conclude, the developments I just mentioned are only a small part of the challenges all of us will be confronted with in the coming years. Data protection authorities (DPAs), but also other stakeholders, will see new ways of collecting personal data at a massive scale being rolled out with great speed.

The COVID-19 crisis is demonstrating the importance of data availability as well as citizens' trust. There is more: it has also unveiled that the protection of personal data is not a problem, it is part of the solution.

We will need all the technological expertise, from DPAs, cyber security agencies, academia, civil society and businesses to create transparency on what is going on, and to ensure the implementation of meaningful safeguards where this is possible.

I am glad to see that contributions on the agenda of this conference will help with the first step - transparency - and I am looking forward to our future cooperation with those working in these fields.

Thank you for your attention.

***