Andrea Jelinek
Chair of the European Data Protection Board

Brussels, 8 April 2020

Dear Ms Jelinek,

Considering the very rapidly evolving developments as regards the use of technology in the fight against the corona pandemic, I deemed it necessary to address the European Data Protection Board again, in follow-up to my letter from last week.

Next to analysing aggregated metadata obtained from telecom providers, Member State authorities are now also studying the use of apps, using Bluetooth signals between mobile phones to detect users who are close enough to infect each other. In recent weeks, we note a prominent role is played by the Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT), an informal collective of researchers developing mechanisms in which Member States seem to be highly interested, and possibly a European standard. Yesterday, the Dutch government announced it would use such a Bluetooth application in the fight against the coronavirus.[1] Other governments, like the Polish government, apparently also encourage the use of such apps.[2] For the time being the use of these apps is on a voluntary basis, but mandatory use is explicitly not excluded by the authorities.
Considering that the technical specificities of such contact tracing apps are still unclear, and that you announced yesterday that the EDPB is developing guidance on tracing tools in the context of the coronavirus outbreak, I have some urgent questions that I would request you to address in upcoming guidelines:

- Within this PEPP-PT collective, researchers are working on two different "tracks": one based on a decentralised mechanism (so-called DP-3T), where the creation and matching of identifiers is done on the terminal device, and where the data does not leave the device and is not stored in a cloud, accessible to authorities. The other track is based on a centralised mechanism, where the data actually does leave the device, and the creation and matching of identifiers is done in a cloud. Considering that the centralised mechanism may be prone to the risk of (later) abuse by authorities, or security deficiencies, and achieves the same goal as a decentralised mechanism, without the potential risk of abuse by authorities, or loss of trust that may endanger uptake throughout the Union, will the EDPB recommend the decentralised systems as European standard, without any central cloud where data are matched and/or stored, fully in line with data protection by design and data minimisation?
- Has the EDPB been in contact with the developers of PEPP-PT? Is it aware of the two different tracks (centralised and decentralised) that the consortium is working on, and the preference of some governments, to opt for the centralised mechanism?
- Does the EDPB agree that full transparency must be given about PEPP-PT, its members, its legal status, its objectives, funding, non-EU partners, and declarations of interest of its members?
- Will the EDPB recommend Member States to use a solid legal basis for the use of contact tracing apps?

[1] https://www.dutchnews.nl/news/2020/04/dutch-see-apps-as-key-to-relaxing-lockdown-tracing-corona-suspects/
[2] https://www.reuters.com/article/us-health-coronavirus-poland-tech/poland-works-on-smartphone-app-to-help-stop-coronavirus-outbreak-idUSKBN21L24R

- Will the EDPB recommend Member States to demonstrate necessity and proportionality of all contact tracing apps, with clear projections that the use of such contact tracing apps, in combination with specific other measures, will lead to a significantly lower number of infected people?
- Will the EDPB recommend Member States to be fully transparent and to publish all details of all contact tracing apps used, so that people can verify both the underlying protocol for security and privacy, and check the code itself to see whether the application functions as the authorities are claiming?
- Does the EDPB agree that obligatory use of contact tracing apps is contrary to our fundamental freedoms in Europe?
- Will the EDPB recommend a concrete sunset clause in national laws regulating these apps?
- Is the EDPB aware of the interest of American companies, such as Palantir, in establishing the software of these applications? Does it agree that there is a significant risk that US government might be able to get access to data processed by any US company or company with presence in the US, through the US Cloud Act and Patriot Act?

Considering the rapidly evolving developments, I hope for an urgent answer from your side and for clear guidelines for the Member States and Commission.

Kind regards,

Sophie in ‘t Veld