Public consultation regarding Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data Adopted on 10 November 2020

This public consultation reply form is aimed at data transfers to the United States.

As a consequence of Schremms II, the United States is considered to have legislation that in the view of the Court, has limitations on the protection of personal data arising from the domestic law of the United States on the access and use by US public authorities of such data transferred from the European Union to that third country, which the Commission assessed in Decision 2016/1250, are not circumscribed in a way that satisfies requirements that are essentially equivalent to those required under EU law, by the principle of proportionality, in so far as the surveillance programmes based on those provisions are not limited to what is strictly necessary. On the basis of the findings made in that decision, the Court pointed out that, in respect of certain surveillance programmes, those provisions do not indicate any limitations on the power they confer to implement those programmes, or the existence of guarantees for potentially targeted non-US persons. The Court adds that, although those provisions lay down requirements with which the US authorities must comply when implementing the surveillance programmes in question, the provisions do not grant data subjects actionable rights before the courts against the US authorities.

The EDPB writes in the Recommendation in paragraph 76:
As an example, US data importers that fall under 50 USC § 1881a (FISA 702) are under a direct obligation to grant access to or turn over imported personal data that are in their possession, custody or control. This may extend to any cryptographic keys necessary to render the data intelligible.

Given the fact that this legislation enbales the authorities in the United States to demand access to or turn over encryption keys (and therefor decryption keys), I wonder if the Use cases 1 to 5 are actually feasible, as they do not seem to take into account that even those encrypted or pseudomised personal data can be decrypted after the United States authorities have demanded the decryption codes on the basis of the above legislation. In other words, these supplementary measures have no effect on transfers to the United States.

Shouldn’t the EDPB be fair enough to either conclude that the only remedy is to wait for the EU and United States authorities to reach an agreement that will have taken away this legislatory impediment of GDPR, or to just advise all data controllers to cease and desist all personal data transfers to the United States full stop?