TrustArc

The Hague Central Station - 1st Floor
Koningin Julianaplein 10
NL - 2595 AA THE HAGUE
The Netherlands
T: +31.6.2493.6643
www.trustarc.com

European Data Protection Board
Rue Wiertz 60
B - 1047 BRUSSELS
Belgium

RE: Public Consultation on Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data

The Hague, 21 December 2020

Dear Chairwoman Jelinek, Dear Andrea,

On 11 November 2020 the European Data Protection Board (EDPB) released the Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (hereafter: the Recommendations) for consultation. TrustArc welcomes the opportunity provided to share it's views on the Recommendations and respectfully submits the comments below for consideration ahead of the final decision.

First and foremost, we would like to thank the EDPB for the guidance provided in the wake of the Schrems-II decision to date, and the announcement that further guidance is still forthcoming. This is not only appreciated, it is also highly necessary. As you will be well aware, the Schrems-II decision created a lot of legal uncertainty, especially when it comes to the free flow of personal data around the world. TrustArc fully recognises the shared responsibility of data exporters and data importers to ensure compliance with the data protection requirements under EU law, but at the same time is concerned that the increased uncertainty will make it especially difficult for small and medium sized enterprises to conduct business with their European counterparts. In this light, we would hope the EDPB stands ready to not only provide further guidance on how to use the various data transfer mechanisms to provide an essentially equivalent level of data protection, but also on the legislation in third countries. It is simply impossible and unaffordable for every single company doing business outside the European Economic Area (EEA) to conduct these assessments themselves. One of the options we would like to suggest, is to create specific white lists, either linked to data type or data subject type in combination with specific laws in third countries where the EDPB considers no supplementary safeguards would be required to allow for the data transfer to take place.

Next, we would call for more clarity on the application of the risk-based approach with regard to the international transfer of personal data. As is clear from the recitals of the GDPR and the legislative debate by the European legislator at the time of creation of the Regulation, the provisions of the GDPR become stricter as the risks to the fundamental rights and freedoms of the data subject increase. In our view, the same logic already

applies to Chapter V GDPR on international transfers: the better safeguards can be provided, the easier the data transfer becomes. It is exactly because risks are taken into account that explicit consent can only be used in exceptional circumstances, whereas if the law of the third country has been deemed adequate (i.e. essentially equivalent) no obstacles are put in place. A risk-based approach should in our view therefore also have a place when assessing the risks related to government interference, even though we appreciate that in light of the CJEU case-law a restrictive approach is desirable. That said, it should be possible to not only consider the consequences of legislation allowing for government interference with the fundamental rights to a private life and data protection, but also the likelihood of such an interference actually taking place.

Without the inclusion of a risk-based approach in the final version of the EDPB Recommendations, a lot of international business will ground to a halt, especially when taking due consideration of Use Cases 6 and 7 as listed in Annex 2. According to the Board, it is apparently not possible to continue to use cloud service providers when data access in the clear is required, nor would it be possible to allow access to data hosted in the EEA to people outside one of the EEA-countries, if far-reaching surveillance laws would exist in the third country. Given the Schrems-II decision and various statements by data protection authorities with regard to U.S. surveillance laws, this would for example mean that data flows between the EEA and the U.S. would become almost, if not completely, impossible. In our view, that position is unwarranted, since it would be detrimental to even the most basic needs of the global digital economy, like the payment of salaries for remote employees or offering round-the-clock customer service.

Allowing organisations to take into account the likelihood of government interference, on top of the requirement to put in place effective supplementary safeguards, would on the other hand allow the digital economy to function, without an immediate impact to the individual's data protection. After all, as soon as the government interference with the fundamental rights to privacy and data protection becomes reality, for example because a subpoena is received or attempts of interception are discovered, the risk assessment changes as well, and would likely mean the data transfer would have to be suspended. We believe that utilizing the accountability principle to ensure that organisations demonstrate compliance with these risk assessment obligations is consistent with the role of that principle.[1]

With regard to Use Cases 6 and 7, the Board concludes "*it is incapable of envisioning an effective technical measure to prevent [government] access from infringing on data subject rights"*. However, the Board does not provide any details of the measures envisioned. We request that in the next version of the Recommendations, more details are provided of the considered options. That way, organizations can still contemplate alternatives that the drafters of the Recommendations may not have considered before.

As a consequence of the strict approach taken to cloud services, a number of commentators have expressed the fear that the Board might be pushing for more data localisation requirements for organisations doing business in the EEA. Similar concerns were voiced in the U.S. during a hearing of the Senate Commerce Committee on 9 December last, where experts agreed data localisation is not a sustainable solution in today's economic climate, especially not between democratic nations. Since the GDPR underlines that "flows of personal data to and from countries outside the Union and international organisations are necessary for the expansion of international trade and international cooperation"[2], data localisation should not be the main solution to the challenges imposed by Schrems-II. In addition, that way consistency would be ensured with the OECD Privacy Guidelines, in

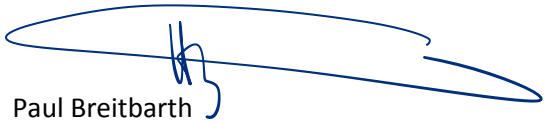
[1] GDPR, recital 85 allows for a similar risk analysis by the controller
[2] GDPR, recital 101

particular Part Four regarding the "Basic principles of international application: Free flow and legitimate restrictions".

We would have welcomed the inclusion in the Recommendations of a definition of what constitutes an international data transfer. Neither the GDPR, nor the CJEU decision, nor the current version of the Recommendations or earlier EDPB guidance include such a definition. This has become more precarious when looking at the draft new Standard Contractual Clauses as presented by the European Commission, which seem to imply any data flows from an EEA based organisation to a non-EEA based organisation subject to the GDPR by virtue of Articles 3(2) and 3(3) GDPR should not be regarded as international transfers. This would for example apply to the situation where an individual would transmit their data to a non-EEA organisation to request more information on an offered product or service. We wonder whether the EDPB agrees with this position and is willing to provide further examples of what it does and does not consider to be an international data transfer.[3] This becomes more relevant should the Board not wish to reconsider their approach to the application of a risk-based approach to international data transfers - if all risks need to be excluded upfront, it would be essential for organisations to also confirm upfront whether or not an international data transfer actually takes place.

We thank you again for your kind consideration of our suggestions. TrustArc remains at your disposal to provide further views or to elaborate on your suggestions, if and when required.

Sincerely yours, on behalf of TrustArc,



Paul Breitbarth
Director, EU Policy & Strategy

[3] We also refer to our letter dated 3 September 2020, requesting further guidance on a similar point