Ms Andrea Jelinek
Chairwoman, European Data Protection Board
European Data Protection Board
Rue Montoyer 30,
1000 Brussels

EPIF Secretariat
c/o Afore Consulting
14B Rue de la Science
1040 Brussels

21st December 2020

Dear Ms Jelinek,

We welcome the public consultation by the European Data Protection Board (EDPB) on its *Recommendations* on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data.

We endorse strong protections for personal data, including when data is transferred to third countries. We believe the Recommendations are key not only to ensuring consistency of the implementation of the CJEU's decision in Schrems II, but also to help data exporters comply with the Court's decision. But we have substantial concerns about some potential interpretations of the Draft Recommendations. In our view , the EDPB is adopting a prescriptive, non-risk-based approach that goes well beyond the requirements of *Schrems II* without giving any consideration to the context of the transfer and the level of risk involved as per the Court's instruction to take the context of a transfer into account.

If adopted in their current form, the *Recommendations* would create serious obstacles for any organisation that uses an online service to process and transfer personal data—including email, hosted applications, or any other online service—to transfers of personal data outside the EU. Organisations would be required to conduct their own costly analyses of the laws and practices of the respective non-EU jurisdictions. This is both unrealistic and disproportionate, in particular for small and medium-sized enterprises, research institutions, and others.

As a result, the *Recommendations* will make it highly risky for EU companies to engage in commerce with non-EU customers or partners, for researchers to share information with foreign colleagues, for companies with non-EU offices or personnel to communicate with them online, or to engage in other routine operational tasks. If adopted, the proposed interpretation of the Court's decision could isolate Europe from the global digital economy; with its obvious negative implications for European competitiveness and innovation. We believe that a more constructive approach is essential to ensure that EU industry leaders as well as SMEs and start-ups continue to have access to cutting-edge and emerging technologies that are available in third countries.

We are also concerned about the potential distortive effects for trade and competition between third country jurisdictions that have been deemed adequate under the GDPR and those jurisdictions where no such positive adequacy decision is in place. EU individuals may lose access to services and face reduced choice about how to live their online life.

We have in particular the following five comments on the draft Recommendations. They should:

1. **Provide a list of regulations considered as not affording a level of protection in the third country that is essentially equivalent to that which is guaranteed in the EEA**
2. **Allow data exporters to take account of the full context of a transfer;**
3. **Propose technical measures that are workable in practice;**

4. **Clarify that contractual measures may provide sufficient safeguards; and**
5. **Make clear that enforcement by supervisory authorities will be measured and appropriate.**

Yours sincerely,

The Co-signatories

Annex 1 – Points for the EDPB to consider

1. ***Provide a list of regulations considered as not affording a level of protection in the third country that is essentially equivalent to that are guaranteed in the EEA***

The Recommendations put on the data exporter the burden of assessing the laws of sovereign States. A legal entity in the Private sector has not the expertise nor the appropriate resources to assess the legal frameworks of third countries. This assessment of third countries regulations should be made by the European Commission or International organisation in a similar way than the OECD provide guidance to the money laundering risk presented by certain States.

This would allow a consistent assessment of those regulations and decrease the level of uncertainty for data exporters.

2. ***The Recommendations should allow data exporters to take account of the full context of a transfer.***

In Schrems II, the Court indicated that data exporters should consider the full context of a transfer when evaluating its legality—specifically, that transfers should be evaluated "in the light of all the circumstances of that transfer" (¶¶ 121, 146) and "on a case-by-case basis" (¶ 134). Several passages in the Recommendations, however, appear to foreclose this contextual approach. For instance, they state that, if the data importer falls within the scope of certain national security laws, the data exporter must use additional technical measures (text box before ¶ 45)—even, presumably, if the data importer has never faced an order under those laws and the data is of no conceivable relevance to national security (e.g., an employee's menu preferences for a holiday party). Other passages similarly suggest that the likelihood that a public authority will ever access the data is irrelevant (¶ 42).

Restricting transfers of data even where the context shows there is virtually no risk to data subjects will harm every corner of the EU economy and society. EU researchers sharing health data with foreign partners to fight COVID-19, EU companies engaging in routine communications with employees outside the EU, and even simple commercial transactions with non-EU entities would all be fraught with substantial risk. Nothing in the Schrems II judgement requires this draconian outcome.

The risk based approach is at the heart of GDPR[1], rather than discourage EU organisations from considering contextual factors, the Recommendations should encourage organisations to take into account the real-worlds risks of a transfer, including the relevance of the data to law enforcement agencies and the likelihood that such agencies would request access to the data. If these real-world risks are low, which they are for most categories of data, the Recommendations should not require organisations to adopt any supplemental measures.

3. ***The Recommendations should propose technical measures that are workable in practice.***

The Recommendations propose a non-exhaustive list of technical measures that data exporters can use to supplement the safeguards in the SCCs. Unfortunately, the Recommendations' case studies on the use of these measures reflect an unworkable and unrealistic view of how these measures operate in practice.

[1] https://eur-lex.europa.eu/eli/reg/2016/679/oj (See Articles 24, 25, 32, 39)

For instance, the Recommendations suggest that organisations can rely on encryption as a safeguard in most cases only if the data never appears in an unencrypted form in the third country and if the decryption keys are held only within the EU (or an adequate jurisdiction) (see, e.g., ¶¶ 79(6), 89(2-3), 84(11)). They also suggest that encryption almost never provides sufficient protection where data is accessible "in the clear" in the third country, including where an EU organisation uses an online service that may process the data in the third country (¶¶ 88-89), or where employees or others in the third country can access the data on a shared IT system (e.g., human resources data) (¶¶ 90-91).

Moreover, because the *Recommendations* state that even remote access by an entity in a third country to data stored in the EU constitutes a "transfer" (e.g., footnote 22, ¶ 13), organisations in many cases would need to apply these technical safeguards to EU-stored data as well. This fact underscores the impracticality of the *Recommendations* and their incompatibility with other important EU interests, such as promoting open global trade and research necessary to protect vital interests (for instance in the context of the COVID-19 pandemic).

At a time when policymakers across the world, including in Europe, are pressing companies to provide greater access to encrypted communications in order to help governments more effectively fight terrorism and other threats, the proposed *Recommendations* would appear to penalize companies for making such access possible. More pragmatically, the *Recommendations'* positions on technical measures would render the SCCs virtually worthless as a transfer mechanism.

There are numerous entirely legitimate activities undertaken every day by organisations both within the EEA and outside of it that require the transfer of personal data to third countries and which represent a minimal risk to the rights and freedoms of the data subjects involved. Many online services that EU businesses rely on today must be able to process the information in unencrypted form in order to work properly; given the nature of the Internet and the global economy, this might entail some processing that occurs outside the EU, irrespective of where the data controller or data processor is based. The *Recommendations* would prohibit EU organisations from engaging in these commonplace and essential business activities, as well as potentially discouraging non-EEA organisations from operating in the EEA, narrowing the scope markets accessible to consumers and inhibiting global competition.

In reality, most EU organisations would not be able to cease these activities entirely while still remaining economically competitive.

To avoid these consequences, the EDPB should revise the *Recommendations* to ensure that the proposed technical measures are workable in practice, and should leave it to data exporters to determine whether any particular measure adequately protects the transferred data particularly taking account of the findings published at our recommendation 1. Most importantly, the *Recommendations* should not prohibit all access to data in the third country; doing so will create barriers to large global enterprises, but also smaller businesses seeking to leverage the full suite of services available on the global economy.

4. ***The Recommendations should clarify that contractual measures may provide sufficient safeguards.***

Although the *Recommendations* propose a non-exhaustive list of contractual measures that can offer additional safeguards, they also include language suggesting that contractual or organisational measures on their own (i.e., without additional technical measures) cannot provide the level of data protection that EU law requires (¶ 48). This position appears to be based on the assumption that the mere theoretical possibility of access by third-country authorities—even if the practical risk of such access is vanishingly small—renders a transfer unlawful.

It could be argued that this position adopts an overly restrictive reading of the *Schrems II* judgement. The Court in *Schrems II* held that transfers of data to third countries should be prohibited only "in the event of the breach of [the SCCs] or it being impossible to honour them" (¶ 137). This language, and similar passages elsewhere in the judgement, suggest that, so long as the data importer does not in fact disclose data to third-country authorities (or, if it does make such a disclosure, that it notifies the data exporter accordingly), then the parties may rely on the SCCs (¶ 139). Under this reading, it is clear that contractual measures alone can provide the additional safeguards needed to safely transfer data to a non-adequate jurisdiction.

To align with the *Schrems II* judgement, the *Recommendations* should remove all language suggesting that contractual measures alone are insufficient safeguards to satisfy EU law. The *Recommendations* should instead articulate several possible contractual / organisational measures that EU organisations may consider when transferring data to a non-adequate jurisdiction, then leave it to data exporters and importers to evaluate which measures are appropriate in context and "in the light of all the circumstances of that transfer" (*Schrems II*, ¶¶ 121, 146).

5. ***The Recommendations should make clear that enforcement by supervisory authorities will be measured and appropriate.***

The Court's holding in *Schrems II* was a major and unexpected development, one that is requiring organisations across the EU to prepare new data transfer impact assessments and, in certain cases, to overhaul aspects of their data transfers. In many cases, these efforts require changes not only to contracts, but also to underlying infrastructure, software, and systems. Undertaking these changes is a complex task that often will involve many different parties, both inside and outside an organisation.

Notwithstanding these facts, the *Recommendations* imply that supervisory authorities should move directly to "corrective measure[s] (e.g. a fine)" if they determine that a data transfer does not comply with the *Recommendations* (¶ 54). This focus on sanctions may lead to a risk that EU organisations to rush through changes to their data transfer practices—making it far less likely that organisations address these issues carefully and precisely.

To avoid this outcome, the *Recommendations* should expressly advise supervisory authorities, when they determine that a specific data transfer does not comply with EU law, to work with data exporters to find acceptable safeguards, and give them sufficient time to implement such solutions. This approach will provide incentives for EU organisations to address these issues thoughtfully, while also encouraging good-faith, collaborative solutions to these quite difficult legal and technical issues

The Recommendations should also define a grace period to implement these new requirements. For companies with an international footprint, adhering to this specific accountability framework will requires resources and investments. At the very least, the implementation timeline should be aligned with the grace period offered for Standard Contractual Clauses.