AMERICAN CHAMBER OF COMMERCE IN POLAND
Spectrum Tower, ul. Twarda 18, 00-105 Warszawa
Tel: +48 22 520-5999, e-mail: office@amcham.com.pl

Warsaw, December 21, 2020

The European Data Protection Board

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

Dear Sir or Madam,

The American Chamber of Commerce in Poland (AmCham) represents over 340 companies doing business in Poland. Our members include all of the substantial US-headquartered companies in Poland as well as many other foreign and domestic companies, which suffer the consequences triggered by the judgment of the Court of Justice of the European Union in the case of Schrems II that reshaped the transfer rules of the personal data from the European Union to third countries, including the United States. Because of the gravity of the situation and undergoing public consultation on Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, AmCham would like to present the position of their member companies below.

On 10 November, the European Data Protection Board (EDPB) issued, for public consultation, its Recommendations on measures to promote compliance with the EU Court of Justice's recent decision in Schrems II. The Court in Schrems II held that organizations that rely on standard contractual clauses (SCCs) to transfer data outside the EU may need to adopt additional safeguards to protect personal data from access by public authorities in third countries.

Although many were hopeful that the EDPB would provide data exporters with a "toolbox" of pragmatic, practical measures that would help them comply with the Court's decision, the proposed Recommendations do the opposite by proposing a prescriptive, non-risk-based approach that goes far beyond the requirements of Schrems II. Rather than follow the Court's instruction to take the context of a transfer into account, the EDPB has adopted a restrictive, absolutist interpretation of EU law that would place insurmountable obstacles to transfers of personal data outside the EU.

If the Recommendations are adopted in their current form, any organization that uses an online service to process and transfer personal data—including email, hosted applications, or any other online service—could face fines up to 4% of its annual turnover, irrespective of whether public authorities in any third country ever access the data in question. They also will require EU organizations to undertake costly analyses of the laws and practices of dozens of non-EU countries (i.e., those not subject to an EU adequacy decision), which will be unrealistic for many small and medium-sized enterprises, research institutions, and other public bodies.

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 countless other routine and necessary operational tasks. If adopted, they will force many aspects of EU commerce and society into a pre-Internet era, and/or isolate Europe from the global economy. The potential negative effects on EU competitiveness, innovation, and society are unprecedented.

Moreover, it is far from clear that all third countries that have an adequacy decision from the European Commission—or indeed that all EU Member States—provide a level of data protection that is "essentially equivalent" to that set out in the GDPR and EU Charter of Fundamental Rights. By focusing only on non-adequate jurisdictions, the Recommendations threaten to create an un-level international playing field for data protection, where data exporters are required to apply different rules to different jurisdictions even where similar levels of data protection exist between them. Such discriminatory treatment of different jurisdictions is also likely to invite retaliation by jurisdictions whose companies are placed at a competitive disadvantage in European markets by the EDPB's actions.

AmCham's view is that, among the points that European and non-European entities and trade associations might wish to raise with the EDPB are the following:

1. 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" and "on a case-by-case basis". 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 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. Therefore, we consider that the compliance checks should be mapped-out based on real risks incurred.

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 judgment requires such a binary outcome.

Rather than discourage EU organizations from considering contextual factors, the Recommendations should encourage organizations to take into account the real-world's risks of a transfer, including the relevance of the data to public authorities and the frequency and likelihood of public authority access to the data. If these real-world risks are low, the Recommendations should not require the organization to adopt any supplemental measures, as set in article 35 of the GDPR.

2. The Recommendation 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 Recommendation's case studies on the use of these measures reflect an unworkable and unrealistic view of how these measures operate in practice.

For instance, the Recommendations suggest that organizations 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). 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 organization uses an online service that may

process the data in the third country, or where employees or others in the third country can access the data on a shared IT system (e.g., human resources data).

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"; organizations in many cases would need to apply these technical safeguards to EU-stored data as well. Such a view makes it so that, implicitly, the EDPB recommendations are in fact more demanding than any data localization obligations, as far as no access from third party countries seems to be acceptable. 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. In the vast majority of cases, the reason companies transfer data to third countries is to communicate and share information with people in those countries. If those people cannot access the information—as the Recommendations would require—there is no point to the transfer. Similarly, 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 organizations from engaging in these commonplace and essential business activities.

In reality, most EU organizations would not be able to cease these activities entirely while still remaining economically competitive. Instead, many would likely turn to other legal mechanisms, such as the derogations set out in Article 49 of the GDPR. Because organizations adopting this approach might transfer data to non-adequate jurisdictions without even adopting SCCs (to say nothing of additional safeguards), this outcome would leave EU data subjects worse off, because their data would be subject to fewer protections than they are today.

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. The Recommendations should not prohibit all access to data in the third country; doing so will discourage organizations from adopting technical measures, such as encryption, that in fact provide meaningful safeguards against unauthorized access.

3. 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 organizational measures on their own (i.e., without additional technical measures) cannot provide the level of data protection that EU law requires. 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.

This position adopts an overly restrictive reading of the Schrems II judgment. 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 honor them". This language, and similar passages elsewhere in the judgment, 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. 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 judgment, 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 measures that EU organizations may consider when transferring data to a non-adequate jurisdiction, then leave it to data exporters and importers to evaluate which additional measures are appropriate in context and "in the light of all the circumstances of that transfer".

4. 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 organizations 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 the underlying infrastructure, software, and systems. Undertaking these changes is a complex task that often will involve many different parties, both inside and outside an organization.

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. This focus on sanctions will lead EU organizations to rush through changes to their data transfer practices—making it far less likely that organizations 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 organizations to address these issues thoughtfully, while also encouraging good faith, collaborative solutions to these quite difficult legal and technical issues.

5. Final remarks.

In order to ensure that international transfers of personal data can be maintained in a way that guarantees legal certainty and the fundamental rights and freedoms of all EU citizens and organizations, AmCham Poland urgently call for:

- The EDPB to understand the need to avoid an overly restrictive approach and to adopt a pragmatic one. It is essential to keep a holistic view in a matter like this one and to balance data protection rights with the economy, scientific research, social well-being, development of other fundamental rights and freedoms and security in the EU.

- The EDPB works towards enabling transfers rather than prohibiting them.

- *The Recommendations* to provide practical and workable guidance that will allow for businesses and organizations to take steps to ensure that they can continue to transfer data in a manner, which respects the essence of EU data subjects' GDPR rights without ignoring other Charter rights of EU organizations. The EDPB should refrain from including impossible standards such "flawless implementation" of certain safeguards, which simply do not reflect the nature of technology or reality.

- *The Recommendations* to explicitly state that GDPR and the ruling in Schrems II permit reliance on a combination of measures and make clear that there is no hierarchy of measures.

- The EDPB to align with the European Commission's pragmatic and more realistic approach for the new set of SCCs.

- The EDPB to recognize that EU and Member States institutions should swiftly negotiate with their United-States counterparts a new mechanism to replace the "Privacy Shield", taking into account all economic and fundamental rights and freedoms, which are not absolute and that the EU and the US share common values and interests, in terms of respect human rights, the rule of law and the cybercrime collaboration.