COMMENTS OF THE AMERICAN BAR ASSOCIATION SECTIONS OF ANTITRUST LAW AND INTERNATIONAL LAW ON THE RECOMMENDATIONS 01/2020 ON MEASURES THAT SUPPLEMENT TRANSFER TOOLS TO ENSURE COMPLIANCE WITH THE LEVEL OF PROTECTION OF PERSONAL DATA

December 21, 2020

The views stated in this submission are presented on behalf of the Antitrust Law Section and the International Law Section. They have not been approved by the House of Delegates or the Board of Governors of the American Bar Association and therefore should not be construed as representing the policy of the American Bar Association.

The Antitrust Law Section and the International Law Section of the American Bar Association (the Sections) recognize the European Data Protection Board (EDPB) for its timely guidance on cross-border data transfer standards, and appreciate the opportunity to comment on the *Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data* (Supplementary Measures Recommendations). The Supplementary Measures Recommendations, together with the *Recommendations 02/2020 on the European Essential Guarantees for surveillance measures* (EEG Recommendations)[1] address issues of the utmost importance to U.S. legal practitioners and the organizations they counsel. Personal data transfers from the European Economic Area to the United States and other third countries are vital for organizations of all sizes and in all economic sectors, and the EDPB's guidance on these issues is critical. To this end, the Supplementary and EEG Recommendations (collectively, the "Recommendations") provide a valuable analysis of the Court of Justice of the European Union's (CJEU) reasoning and conclusions in *Schrems II*,[2] as well as detailed recommendations on measures that data exporters and importers may need to adopt to supplement standard contractual clauses and other transfer mechanisms.

The Sections recognize the central role that effective enforcement plays in data protection. However, we respectfully suggest that the EDPB adopt a policy that encourages supervisory authorities to use their enforcement powers to establish fair and predictable standards while fully

[1] The Antitrust Law Section is the world's largest professional organization for antitrust and competition law, trade regulation, consumer protection and data privacy as well as related aspects of economics. The International Law Section (ILS) is the American Bar Association section that focuses on international legal issues, the promotion of the rule of law, and the provision of legal education, policy, publishing and practical assistance related to cross-border activity. Together, the Sections' members include private practitioners, in-house counsel, attorneys in governmental and inter-government entities, and legal academics, and represent over 100 countries.

[2] Case C-311/18, *Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems*, (July 16, 2020) (Eur. Ct. Justice).

protecting data subjects' fundamental rights.[3] In particular, the Sections are concerned that organizations could follow the Recommendations – diligently, in good faith, and under the advice of qualified counsel – and still be exposed to fines by supervisory authorities who determine that supplementary measures do not meet EU standards.[4] The legal analyses required by the Recommendations, described below, are extraordinarily complex, and organizations and supervisory authorities can easily reach different conclusions regarding the application of legal frameworks in third party countries and whether supplementary measures to address concerns raised by those frameworks are adequate. Indeed, even a conservative and pragmatic interpretation could still lead to practical challenges for organizations. Under these circumstances, it is appropriate for supervisory authorities to use enforcement – and enforcement discretion – to help clarify standards and identify practices that fall short of these standards.[5]

To this end, we suggest that the EDPB adopt a policy of encouraging supervisory authorities to use a range of measures at their disposal to effectively achieve general deterrence goals while considering principles of fairness in dealing with individual organizations, consistent with GDPR article 83(2). Where newly developed rules may be ambiguous, the Sections encourage the EDPB to use alternative measures to clarify enforcement standards. At the same time, the EDPB should adopt an enforcement policy that allows discretion to forbear from issuing fines against organizations that (1) do not have prior violations relating to data transfers; (2) can demonstrate that they have thoroughly analyzed their obligations under the Recommendations and followed them in good faith; and (3) take prompt and effective steps to address concerns raised by the relevant supervisory authority or authorities. This is *not* to suggest that such good-faith efforts should relieve organizations from potential liability under the General Data Protection Regulation (GDPR), nor are the Sections recommending that the EDPB consider a policy in favor of limiting

[3] The Sections note that this comment does not explore other significant issues raised in the Recommendations due to the brief time allowed for public consultation. *See, e.g.*, Supplementary Measures Recommendations at paragraphs 87-91. Specifically, in Use Cases Six and Seven, the EDPB indicates it has initially found no effective technical safeguards. These scenarios include data processing in the clear by cloud service providers (i.e., unencrypted processing) or remote access and use of data in the clear from a third country for business purposes, such as human resource processing.

[4] *See* Supplementary Measures Recommendations at paragraph 54 ("The competent supervisory authority may impose any other corrective measure (e.g. a fine) if, despite the fact that you cannot demonstrate an essentially equivalent level of protection in the third country, you start or continue the transfer.")

[5] Examples of how U.S. privacy and consumer protection authorities use a variety of non-monetary enforcement tools to achieve similar goals may be instructive. In particular, the Federal Trade Commission often uses warning letters and closing letters to clarify standards and articulate enforcement priorities. *See, e.g.*, Fed. Trade Comm'n, FTC Warns Data Broker Operations of Possible Privacy Violations (May 7, 2013), https://www.ftc.gov/news-events/press-releases/2013/05/ftc-warns-data-broker-operations-possible-privacy-violations; Fed. Trade Comm'n, About FTC Warning Letters, https://www.ftc.gov/news-events/media-resources/truth-advertising/about-ftc-warning-letters (last visited Dec. 2, 2020). The FTC applies this approach in areas that combine significant risk to individuals with rapidly developing practices. *See* Fed. Trade Comm'n, FTC Coronavirus Warning Letters to Companies, https://www.ftc.gov/coronavirus/enforcement/warning-letters (last visited Dec. 2, 2020).

remedies other than fines. As standards in this become better developed over time, the EDPB could consider adapting its enforcement policy accordingly.

Under the Recommendations, organizations have substantial obligations to assess the data importer's legal system under the European Essential Guarantees.[6] These obligations include fully mapping data flows under proposed transfers, determining how the domestic legal system of the third country, including requirements to disclose personal data to public authorities, applies to transferred personal data; providing greater transparency about public authorities' data collection practices than the authorities themselves provide;[7] and, once the third country's legal system is fully analyzed, mapping that system to the EEGs and identifying whether supplementary measures will suffice to meet the protections set forth in the EEGs.

The legal analysis that the Recommendations envision is complex and uncertain. As the EDPB recognizes, the EEGs "require a certain degree of interpretation, especially since the third country legislation does not have to be identical to the EU legal framework."[8] Organizations must evaluate laws and regulations that are seldom encountered in the private sector and may be subject to no formal guidance or interpretation by agencies or courts. If an organization's good faith analysis could be re-evaluated by a supervisory authority, it is possible that fines could be imposed, without sufficient justification in the language of the GDPR itself, or sufficiently taking into account the practical consequences. The experience of the European Commission and the U.S. government in developing the EU-U.S. Privacy Shield Framework underscores the difficulty of such an analysis. Experts from a broad array of U.S. government agencies and the Commission arrived at an analysis and data transfer mechanism that both sides believed to satisfy the "essential equivalence" standard articulated by the CJEU in *Schrems I*.[9] The CJEU rejected this analysis.

Organizations face the same potential fate as they devise, evaluate, and implement supplementary measures. However, these organizations have less expertise and more limited resources than the Commission and the U.S. government; and these organizations may be subject to significant financial penalties if supervisory authorities and courts disagree with them.

---

[6] *See* EEG Recommendations at paragraph 8 ("[T]he European Essential Guarantees form part of the assessment to conduct in order to determine whether a third country provides a level of protection essentially equivalent to that guaranteed within the EU . . .").

[7] *See* Supplementary Measures Recommendations at paragraphs 30-38, 99-101.

[8] EEG Recommendations at paragraph 49.

[9] *See* Commission Implementing Decision 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield, at paragraph 137.

The Sections respectfully suggest that fines are not appropriate for organizations that conduct the required legal analysis and adopt supplementary measures in a good-faith effort to meet the requirements outlined in the Recommendations. To satisfy the Recommendations, organizations will have data maps; assessments of the effectiveness of their transfer tools against the EEGs; and, potentially, technical, contractual, and procedural measures to supplement their transfer mechanisms. These steps not only provide robust safeguards for data subjects' rights but also strongly discourage organizations from engaging in Article 46 data transfers in the first place unless they have undertaken a risk assessment, have adopted strong supplementary measures, and possess the documentation to support the sufficiency of these protections.

Imposing significant fines after organizations provide the above safeguards and supervisory authorities order other remedies would do little to advance the protection of fundamental rights. Such fines, however, could impose substantial costs on data exporters (and potentially on data importers). Accordingly, the EDPB should adopt an express recommendation of forbearance from fines (but not other remedies) for organizations that undertake the Recommendations' requirements but nonetheless fail to persuade the competent authority that their measures provide an essentially equivalent level of protection to EU law.

* * *

In conclusion, the Sections appreciate the opportunity to provide these comments and hope that our brief input encouraging fair and predictable outcomes for organizations that strive to meet the Supplementary Measures Recommendations' requirements will serve as a basis for constructive dialogue and serious consideration of these important matters.