Before the

European Data Protection Board

Brussels, Belgium

Internet Association's Comments in Response to Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data.

Internet Association ("IA") appreciates the opportunity to respond to the "European Data Protection Board's ("EDPB") recommendations on measures that supplement transfer tools to ensure compliance with the European Union ("EU") level of protection of personal data" ("EDPB Recommendations/Guidance")[1] in light of the Court of Justice of the European Union's ("CJEU") judgment in *Data Protection Commissioner v. Facebook Ireland LTD, Maximilian Schrems* ("Schrems II").[2] IA member companies take the privacy of personal information seriously and respect the EU's efforts to strike the appropriate balance between protecting EU citizens under the General Data Protection Regulation ("GDPR") and EU surveillance laws while still allowing for efficient and effective cross-border data flows. IA member companies support all consumers' personal information being safeguarded and encourage effective international regulations and guidance that enhance data flows amongst countries such as the U.S. and the EU. IA submits these comments in response to the EDPB's Recommendations that would negatively impact the free flow of data without providing meaningful privacy protections to EU consumers. IA hopes these comments will inform the EDPB's efforts to provide recommendations around third country cross border data flows.

IA represents over 40 of the world's leading internet companies[3]and is the only trade association that exclusively represents leading global internet companies on matters of public policy. IA's mission is to foster innovation, promote economic growth, and

[1] Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (released November 11, 2020).

[2] CJEU judgment of 16 July 2020, Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems, (hereinafter C-311/18 (Schrems II)), second finding.

[3] IA Member Company List: https://uk.internetassociation.org/our-members/.

empower people through the free and open internet. We are firm believers in the benefits that technology brings to everyday life and the economy, and for the potential that internet innovation has to transform society for the better.

The internet is a borderless medium and the movement of electronic information enables virtually all global commerce. Every sector of the economy relies on information flows, from manufacturing, to services, to agriculture. We appreciate that the EDPB may be acting according to the CJEU's instructions to provide further guidance to what is required under the GDPR's Article 46.2 "additional safeguards", "additional measures", or "supplemental safeguards", however the Recommendations put forth for data transfers between the EU and third countries are overly prescriptive and focused on technical measures. IA believes that the EDPB could accomplish its objectives by adopting a risk-based approach that would avoid hindering the EU from working collaboratively with countries outside its borders and creating insurmountable barriers for global companies of all sizes engaging in cross border data flows with the EU.

I. The EDPB's Approach to Guidance Should Support A Risk-Based Approach to Cross Border Data Flows.

In contrast to the findings in the *Schrems II* judgment, the EDPB's Recommendations take a prescriptive, one-size fits all approach. The EDPB deviates from a "case-by-case" risk-based approach to personal data transfers amongst countries, and instead lays out six steps and technical standards that must be implemented in a specific way to provide "equivalent" protections to EU citizens' personal data. For example, if a data importer is located in a country that falls outside of the EU's acceptable or equivalent national security protections, the data exporter is required to implement additional technical measures.[4] The measures are required regardless of whether the data importer has ever been subject to a government inquiry or whether the data being collected would ever be subject to national security laws. There is no accounting for whether the information is as simple as digital advertising or information that may be subject to a foreign public authority's review. Furthermore, the burden remains on the data exporter to thoroughly investigate "with due diligence" all third countries laws, legislation, or public authority oversight, which adds increasing difficulty under these

[4] EDPB Recommendations at ¶ 45.

prescribed conditions for personal data flows to continue across the globe.[5]

Limiting personal data transfer between the EU and other countries will drastically change the EU economy and society. If the EDPB's Recommendations are immediately implemented it could also impact the EU's ability to contribute and receive instrumental research around the COVID-19 virus. Currently, many companies and independent researchers around the world are sharing health data and trial outcomes with foreign partners in hopes of finding timely cures to this international pandemic. Given the EDPB's new guidance companies located in the EU and that work with EU member states could encounter substantial risk just based on internal employee communications about new cures, vaccination trials, or distribution mechanisms. Surely, the EDPB did not intend this outcome, so it should reevaluate some of its prescriptive requirements within these Recommendations.

As we have seen over time, context is critically important to any long-lasting and forward-thinking legislation or regulation. IA encourages the EDPB to take into account real world factors and allow for a risk-based approach to ensure the protection of EU citizens' personal data during cross border data flows. Without providing flexible solutions for protecting EU citizens data, companies outside the EU will be forced to make strenuous decisions about their relationships with EU businesses and EU companies will simultaneously face extreme financial burdens to comply with these Recommendations. Both will result in negative consequences for EU consumers, thus there is a need to reassess the EDPB's methods for providing EU protections outside of their borders. The EU should endorse a risk-based and adaptable approach to ensure the protection of EU citizens' personal data.

[5] EDPB Recommendations at ¶ 42.

II. The EDBP Should Clarify That Standard Contractual Clauses ("SCCs") Are Able to Provide Sufficient Protections to Personal Data During Cross Border Data Flows Without Additional/Supplemental Measures.

Within Step 4 of the EDPB's Recommendations, there is some indication that "contractual and organisational measures alone will not overcome access to personal data by public authorities of the third country."[6] This statement seems to be made assuming that the mere possibility of a public authority being able to access an importer's data would indicate that the third country's law was not up to the same standards of the EU's protections of personal data. However, this presumption seems to be contrary to the CJEU's interpretation of SCCs' protection of an EU citizens' personal information. Instead the *Schrems II* decision indicates that so long as the data importer does not share the EU citizens data with the third country public authority the SCCs would remain in place and valid without any additional technical measures or supplemental procedures.[7] Therefore, it would seem that so long as a SCC had the appropriate mechanisms in place to safely transfer data amongst countries the SCC alone could provide EU citizens with the needed protections in both countries without additional technical or supplemental measures.

IA would support the EDPB providing companies and organisations with SCCs examples that would allow an adequate transfer of data between the EU and a third country. By providing data importers and exporters with these types of recommendations companies can efficiently and effectively implement protocols and SCCs that address the EDPB and CJEU's concerns without having to completely redesign their systems or consider ending ties with EU businesses. IA would also suggest that the EDPB consider eliminating references within its Recommendations that SCCs alone are inadequate methods of protecting EU citizens' personal data without some type of supplemental contractual measure. This will allow both data importers and exporters to assess the circumstances at hand and make the necessary adjustments to their SCCs to provide equivalent protections to EU citizens' personal data.

[6] EDPB Recommendations at ¶ 48.

[7] *Schrems II* at ¶¶ 137 & 139.

III. The EDPB Should Provide Technical Measures That Are More Amenable to Real World Applications.

In the case where technical measures would be a useful supplemental measure for businesses to adequately protect EU citizens' personal data, IA would recommend that they are workable in practice. For example, the EDPB's Recommendations suggest encryption as a viable supplemental safeguard. However, it is only permitted if (1) the data cannot be decrypted in the third country by the data importer and (2) the decryption keys are only contained within the EU (or another adequate jurisdiction).[8] Additionally, the Recommendations indicate that encryption may not be a sufficient solution when data is somewhat accessible to third countries, including EU entities that process data in a third country or where third country employees have access to EU citizens personal data.[9] Thus, a data importer in a third country would never be able to process unencrypted data due to the technical measures put in place even if it was part of their core services.

These impractical technical measures will specifically impact SMEs using U.S. cloud providers to operate online stores: smaller companies have greatly increased their participation in international trade using online services based in the U.S. to connect with customers and suppliers, provide information, take and place orders, and facilitate the delivery of products and services. The restrictive use cases provided for in the EDPB Guidance mean smaller companies that have benefited from greater connectivity with customers and suppliers through online platforms will be seriously harmed if they cannot rely on SCCs because implementing workable technical safeguards is not sufficient.

Instead of EDPB's Recommendations providing impractical examples for data exporters and importers subject to the Guidance, it should instead allow EU data exporters to use their good-faith business judgment relying on a risk-based approach to determine what measures are required to protect EU citizens' personal information, as required under the GDPR. The EDPB's Recommendations should allow for flexible use cases and potentially after a few years provide effective examples of implemented and adaptable technical solutions that can work alongside SCCs or provide SCCs that work as a standalone agreement for cross-border data flows.

[8] EDPB Recommendations at ¶ 79(6), 89(2-3), 84(11).

[9] *Id*. at ¶ 88-89.

IV. Conclusion

IA appreciates the EDPB's efforts to protect EU citizens' personal data throughout cross border data transfers. IA members' companies do their best to also implement effective mechanisms to protect all users' privacy rights while using their services. We recognize the importance of international cross border data flows and know the critical role that agreements like those between the EU and U.S. (aka Privacy-Shield Safe Harbor) make. IA encourages all stakeholders to come to the negotiating table to discuss the issues presented in these Recommendations and find amenable, productive ways to maintain transatlantic data flows. It is with compromise and robust discussion that the EU will be able to implement workable and risk-based Recommendations for protection of EU citizens personal data. IA thanks you for your consideration of our thoughts around the EDPB's Recommendations.

Internet Association

21 December 2020