British American Business

Finsgate, 5-7 Cranwood Street, London, EC1V9EE
Tel: 020 7290 9888
52 Vanderbilt Avenue 20th Floor, New York, NY 10017
Tel: 212 661 4060
www.babinc.org

The European Data Protection Board
Rue Wiertz 60
B-1047 Brussels
Belgium

21 December 2020

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

We are writing on behalf of BritishAmerican Business (BAB) in response to the European Data Protection Board (EDPB)'s public consultation on its recent Recommendations on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data.

BritishAmerican Business is the leading transatlantic trade association created as a result of the merger between the British-American Chamber of Commerce in the United States (U.S.) and the American Chamber of Commerce in the United Kingdom (UK).

We represent many of the leading British and American firms that are responsible for a significant portion of the overall transatlantic trade investment and jobs in the UK and across the whole of the European Union (EU).

We are committed to strengthening this economic relationship to the benefit of the economies on both sides of the Atlantic. As part of our work, we support policies and actions that protect and enhance the environment for transatlantic trade and investment on behalf hundreds of transatlantic companies with operations across the UK, the US, and the EU.

With that, our members based in the UK follow EU policy closely and welcome any efforts made to strengthen growth and innovation in the EU.

Our members are committed to data privacy and the sensible processing of data. We welcome the efforts made to remove the uncertainty for transatlantic companies which the recent European Court of Justice (ECJ) decision on the Privacy Shield has generated.

With the UK due to become a third party to the EU, it is vital that companies with presence in the EU understand how to transfer data across borders lawfully and practically. This is particularly important as many of our members, while active across the whole of the EU, have their European headquarters in the UK.

Additionally, the UK Government is currently seeking adequacy decisions from the European Commission under both the General Data Protection Regulation (GDPR) and Law Enforcement

Directive, which, if secured, will mean that data privacy guidelines coming from the EU will also be implemented by companies based in the UK.

The lawful flow of personal data is one of the cornerstones of the transatlantic economy. Businesses of all sizes and in sectors as diverse as healthcare, transportation, hospitality, retail, information technology, logistics, and finance, among others, rely on globally delivered services and the ability to transfer data to conduct cross-border commerce.

In the absence of the EU-U.S. Privacy Shield, which was used by thousands of transatlantic companies to transfer and process data, Standard Contractual Clauses (SCCs) remain the only legal mechanism available – and in fact 94% of companies transferring personal information to the United States use SCCs.[1]

We were therefore pleased to see the ECJ uphold the validity of SCCs as a way to continue cross-border data transfers and we welcome the EDPB's efforts to provide additional guidance and clarity.

However, we would like to use this opportunity to draw attention to several issues in the Recommendations which we believe would harm the transatlantic business environment, and in particular cross-border investment by making cross-border data transfers more difficult and, in many critical cases, even impossible.

1. First and foremost, the steps which a company would have to take are extremely onerous, requiring it to do a complex analysis of a country's national security laws. This process is cumbersome to all businesses but will particularly impact smaller companies with fewer resources and expertise to dedicate to it. This will lead to an inability to continue providing digital and digitally-enabled goods and services beyond Europe and access new markets, harming their competitiveness and, in turn, harming the competitiveness of the transatlantic economy.

2. Secondly, we note that the approach laid out in the Recommendations is not risk-based, applying to all personal data including low-risk data such as name and work email addresses. The practical implications of this will be severe. Many companies operating across the Atlantic store human resources and other business operational data in the U.S. The application of the Recommendations would lead to an inability to lawfully perform day to day operations, including those as basic as sending intra-company emails or other messages. It is worth noting that the GDPR was introduced utilising a risk-based approach, which made allowed for efficient implementation. We recommend for that same approach to be mirrored in these regulations so that low-risk data, such as employee data, can be transferred where needed.

3. Thirdly, we are worried about the overreliance on impractical technical measures. To transfer even low-risk data out of the EU to a jurisdiction without an Adequacy Decision, that data must be encrypted, and the decryption keys must be stored in the EU. This would be highly impractical to implement and would lead to many companies being in breach of GDPR for conducting day to day operations.

4. Finally, the practical result of these Recommendations would be a drastic increase in data localization in Europe. Under the EDPB's recommendations, everyday transfers of personal information may result in violations of the GDPR. This would limit vital activities such as communications between colleagues across borders, researchers and public health officials

[1] https://www.businesseurope.eu/publications/schrems-ii-impact-survey-report

sharing data to fight COVID-19, or financial services firms leveraging global platforms to detect and combat fraud and money laundering. Localization requirements also increase data hosting costs by 30 to 60% and impact free speech, social mobility, and civic engagement by restricting information availability.

The concerns above are shared by our partners in the business community in both the UK and the EU. They reflect our joint efforts to ensure that data privacy compliance is practicably feasible, ensures data connectivity between leading economies, and does not harm our efforts to play a part as an international business community in the growth, innovation, and stability on both sides of the Atlantic.

We welcome the opportunity to express our views. We appreciate any efforts to help our community to continue transferring data with confidence, compliant with the European Court of Justice's ruling and the GDPR framework, and in a feasible way.

Finally, with view to the importance of the transatlantic economic corridor, we are hopeful that European and American authorities will successfully agree on a framework for an enhanced EU-U.S. Privacy Shield, to allow for simpler compliance with European data privacy provisions.

Ensuring the secure and free flow of data between economic partners will be an important element in our joint efforts to recover from the crisis and prepare our economies for the future.

BritishAmerican Business stands ready to work with the EDPB on these vital issues. We appreciate your consideration of our submission.

For further information, please contact:
Andrei Cazacu
acazacu@babinc.org