Amcham Croatia position on European Data Protection Board (EDPB) Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the European Union (EU)

The ability to transfer data internationally is an inherent part of the global economy's operation and social exchanges. In fact, organisations of all sectors within the EU, whether public or private, EU multinationals and SMEs, heavily rely on the possibility to transfer personal data to third countries in order to be able to provide their services in the EU and around the world. Today, practically no organisation, irrespective of sector, would be able to do business, let alone take part in international trade, without the ability to transfer data cross-borders. **Data flows play an invisible but structural role in the delivery of products and services that EU citizens rely upon in day-to-day life.**

The Recommendations fail to have regard to this reality and that the overly burdensome and prescriptive approach it sets out is likely to have very far-reaching negative impacts on the fundamental rights and freedoms of EU citizens and of EU organizations and on the EU economy and way of life more generally.

The Recommendations fail to consider the GDPR's risk based approach and do not distinguish categories of data; therefore, server load, service metadata, configuration checks, or logs that may contain identifiable information would get the same treatment as sexual orientation, political affiliation, or religion data. The risks inherent to those to the rights and freedoms of natural persons are very different. Also, the Board eliminates the possibility to take the likelihood into account, which is a fundamental part of any risk assessment in line with widely accepted international standards and GDPR's own recital 75.

The Recommendations reflect a failure to take into account any of the other rights and freedoms enshrined in the Charter of Fundamental Rights as well as other legitimate interests, including the present and future of the EU economy, the social well-being and health of EU citizens and EU security that requires a global approach.

The Recommendations are overly prescriptive and place a heavy burden on organisations that may not always have the capability to achieve and maintain compliance. For example, the roadmap requires a detailed analysis of the characteristics of every transfer, an assessment of all applicable local laws - this is a highly complex assessment requiring specialist multi-jurisdictional legal advice, to be routinely re-evaluated, which many businesses will not have available to afford. In

addition, the cost of implementing some of the actual recommended safeguards would make many businesses unviable or prohibitively onerous.

The Recommendations undermine and will damage EU businesses and EU citizens' rights and opportunities by failing to adopt a proportionate and risk based approach and by not acknowledging the importance of other fundamental rights and freedoms, including the right to freedom of expression and information (Articles 11 and 7 of the Charter) and freedom to conduct a business (Article 16 of the Charter). The right to the protection of personal data must co-exist and be balanced against these other fundamental rights.

The Recommendations specifically call for additional supplemental measures that make access from a technical perspective impossible or ineffective in the third country. In practice, this would prohibit any EU business from relying on many global service providers that provide communication services (e.g., email, videoconferencing, posts, etc.) or money transfers that must access communications or related personal data to deliver these services.

The Recommendations essentially require organisations to implement specific technical measures in order to rely on the SCCs in many cases and preclude reliance on organisational, contractual and other measures. In doing so, the Recommendations depart significantly from the wording of the GDPR and the CJEU *Schrems II* ruling – neither of which prioritised technical measures over and above other types of measures, such as organisational, contractual or legal. Also, the proposed technical safeguards are overly stringent when it comes to encryption key management controls, mandating that data exporters should manage their own encryption keys. This may raise unintended concerns over potential data loss and may not always be the most appropriate solution from an information security standpoint.

For additional information, please contact:
American Chamber of Commerce in Croatia
Andrea Doko Jelušić,
Executive Director
T: 01 4836 777
E: andrea.doko@amcham.hr