Statement on ECJ Schrems ruling, the EDPB guidance and the new SCCs

Zagreb, December 2020.

AmCham

American Chamber of Commerce in Croatia

Američka gospodarska komora u Hrvatskoj
## Contents

Statement on ECJ Schrems ruling, the EDPB guidance and the new SCCs ................................................. 3

**Introduction** ............................................................................................................................................ 3

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) ............... 4

Amcham Croatia position on new SCCs ................................................................................................. 5

Conclusion and recommendations ........................................................................................................ 6
Statement on ECJ Schrems ruling, the EDPB guidance and the new SCCs

Introduction

Amcham Croatia would like to express its concerns on the possible adverse consequences of the Court of Justice of the European Union’s decision in the Schrems II case. International transfers of personal data are at the heart of European economic exchange, growth and innovation. Organisations of all sectors within the European Union (EU), whether public or private, big EU multinationals, start-ups or smaller organisations, 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. The invalidation of the EU-US Privacy Shield and the recent doubts raised with regards to the possibility to rely on Standard Contractual Clauses (SCCs) and Binding Corporate Rules (BCRs) could lead to a situation where international transfers of personal data would be made impossible. Amcham Croatia therefore urges all parties involved to adopt a balanced position on the implementation of the CJEU decision.

In its decisions, the CJEU invalidated the European Commission adequacy decision "Privacy Shield“ which enabled EU-US data flows, due to concerns over US surveillance law. However, the Court confirmed the validity of the Standard Contractual Clauses, which enable transfers to any country, including the US, and which, depending on the situation of each transfer, organisations need to consider additional safeguards and supplementary measures to the protection offered by the SCCs. The Court placed the burden on EU organisations to assess whether surveillance legislation of all third countries, i.e., not just the US, for example the UK post 2020, India, Brazil and Australia, guarantees adequate protection if compared to EU laws and practices.

The situation is even more critical given that companies are already or might potentially be the targets of complaints putting into question the possibility to rely on SCCs and BCRs for international transfers to the United States. Such a calling into question could lead to the halt of international transfers of personal data all together, which would negatively affect the whole European economy by isolating EU businesses, public administration and citizens. In fact, European companies are part of the global economy and rely on or offer services and structures requiring the possibility to transfer data (cloud storage, social networks for marketing or for enabling social international interactions, clinical trials, or call centres providing support to European and international consumers). Such a restriction of international transfers, beside putting the economy at risk, seems to go against core European values, including the fundamental freedom to conduct a business as enshrined in Article 16 of the Charter of Fundamental Right of the European Union. The social
impact to citizens will be immense with restrictions on communications, disruptions to daily life and access to information.

By shifting the responsibility to assess the level of protection of a third country, the CJEU is putting European companies, especially smaller organizations who may lack the human and financial resources to do so efficiently, in an unfair position. This is all the more true considering that the Commission, with its vast resources, has only been able to conduct this kind of assessment in more than 20 years for a few number of countries or territories and, as per the CJEU, this assessment was wrong on two occasions.

European stakeholders have proven global leadership on data protection issues, but they need to take responsibility for providing clear guidance on how to move forward in a way that allows data flows to continue while protecting data and preserving the security relationship.

**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.

Amcham Croatia position on new SCCs

Amcham Croatia acknowledges the Standard Contractual Clauses (SCCs) are a step towards legal certainty. In today’s world, data flows are as ever present as electricity, they play an invisible but critical role in our everyday lives, from streaming tv shows,
online bookings to the most complex pharma testing. Decisions taken on the future of such issues need to be taken in public, factoring in a wide range of views and the impact data flows have on all rights under the Charter.

Amcham Croatia welcomes the detail and level of effort the Commission has put into developing new SCCs that are pragmatic, flexible and update data subjects rights in accordance with GDPR. The new SCCs are a welcome effort to modernise and update the instrument as well as filling the legal limbo left by the recent Schrems II ruling.

**Amcham Croatia furthermore praises the risk-based approach as a key to a harmonised and sustainable transfer mechanism.** This provision of the draft SCCs is a pragmatic recognition of the factual circumstances and individual context of data transfers that need to be assessed based on associated risks on the ground and in practice. This is key to ensuring organisations can take their unique circumstances, business operations and type of data into account when considering international transfers. This is consistent with the GDPR and the CJEU which is focused on protecting against real damage, risk and not theoretical possibilities.

Schrems II has introduced a great deal of legal uncertainty for European businesses. The long term solution to the challenges raised by the ruling will need a political solution. These SCCs are a welcome step towards legal direction but now more than ever it is important for the EU and the US to come together and reinvigorate the transatlantic relationship.

**Conclusion and recommendations**

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 Croatia urgently call for:

- The European Commission, to swiftly negotiate with their United-States counterparts an enhanced EU-U.S. Privacy Shield framework, taking into account all economic and fundamental rights and freedoms. We urge the governments to prioritize and maintain momentum on this work even during the US administration transition period. Negotiations should aim to provide both short-term stability for companies facing significant uncertainty as well as a long-term, durable basis for cross-border personal data flows.
- The EU DPAs under the EDPB umbrella to implement the CJEU ruling in a consistent and coordinated way and to collaborate in accordance with the GDPR consistency and cooperation mechanism. Significant divergence in how the ruling is interpreted will lead to widespread business uncertainty across many sectors of the economy.
- 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 to revisit the immediate effect of these Recommendations to consider the appropriate measures to review the contributions it will be receiving during the public consultation period and provide data controllers the necessary time to implement the Recommendations.
- The EDPB to consider GDPR’s risk-based approach, which is essential to any risk management strategy.
- The EDPB to revisit its Recommendations in order to provide practical and workable guidance that will allow for businesses and organisations 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 organisations. The EDPB should refrain from including aspirational standards such “flawless implementation” of certain safeguards which simply do not reflect the nature of technology or reality.
- The EDPB 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 or that at the very least strikes a better balance between privacy and security from a technological standpoint.
- The EDPB to align with the European Commission’s pragmatic and more realistic approach for the new set of SCCs.
- We encourage the Commission to retain and integrate the risk based approach in the final version of the SCCs. This can be assisted by including direct references to the accountability principle of the GDPR.
- The Commission to consider how all stakeholders such as public health bodies, public authorities, law enforcement, consumer groups, academics and research bodies, not just DPAs and industry, can come together to reflect and explain the role data flows play in underpinning our modern lives.
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