AmCham EU
SPEAKING FOR AMERICAN BUSINESS IN EUROPE

Consultation response

AmCham EU input to the EDBP consultation on Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data

AmCham EU speaks for American companies committed to Europe on trade, investment and competitiveness issues. It aims to ensure a growth-orientated business and investment climate in Europe. AmCham EU facilitates the resolution of transatlantic issues that impact business and plays a role in creating better understanding of EU and U.S. positions on business matters. Aggregate U.S. investment in Europe totalled more than €3 trillion in 2019, directly supports more than 4.8 million jobs in Europe, and generates billions of euros annually in income, trade and research and development.

American Chamber of Commerce to the European Union
Speaking for American business in Europe

Avenue des Arts/Kunstlaan 53, 1000 Brussels, Belgium • **T** +32 2 513 68 92
info@amchameu.eu • amchameu.eu • European Transparency Register: 5265780509-97

The American Chamber of Commerce to the European Union (AmCham EU) appreciates the attempt to provide a roadmap for the implementation of the new standard contractual clauses (SCCs) and the EDPB's public consultation on the Recommendations 01/2020 to collect feedback on the supplementary measures, given that this is an important issue that affects thousands of businesses. From small and medium-sized enterprises (SMEs) to international corporations, business relies on international data transfers on a day-to-day basis. Although we appreciate the desire to issue recommendations that are helpful, businesses will struggle with the EDPB's sharp focus on technical measures, specifically the conclusions about transferring unencrypted data out of the EU and onerous requirements for risk assessments.

AmCham EU members support the purpose of the Recommendations to protect rights and privacy of citizens. However, rather than directly addressing concerns with the foreign governments that control data protection legal regimes, the recommendations shift the responsibility and burden of assessing and supplementing the essential equivalent protection of legal systems to the private sector in a manner that goes beyond the Schrems II ruling of the Court of Justice of the European Union (CJEU). While the court's decision described the responsibilities of both supervisory authorities and data exporters, the EDPB guidance suggests that the burden falls entirely on the latter. The Recommendations should acknowledge that much of this responsibility naturally belongs to public apparatuses designed to tackle international and transatlantic law issues. Placing too great of an onus on the private sector would inevitably lead to inconsistent conclusions and differing protectionary approaches.

We are concerned that the EDPB guidance goes beyond both the general data protection regulation (GDPR) and the CJEU's decision in Schrems II in additional respects. We would urge the EDPB to recognise more explicitly that the application of safeguards should be risk-based, reflecting the type and volume of personal data (including whether or not it includes special categories of data), the type of government surveillance requests and access to which a multinational may be exposed, etc. This is consistent with the overall positioning of the GDPR and the modern privacy jurisprudence to ensure adequate and robust protection of stakeholders' personal data while maximising efficiencies in technology services rendered to these data subjects – whether they are consumers, employees or others.

Some elements of the recommendations, if confirmed, would place an extreme burden on businesses of all sizes and sectors trying to conduct business with the US. A seamless system for the transfer of data across borders is essential for competitiveness and innovation. As currently drafted, we understand firms will be unable to send unencrypted data to the US. It also can be read as closing all avenues for state of the art and affordable cloud computing and remote access to data, which are critical to EU businesses. The practical impact of the requirements will also have a negative impact on operational resiliency if firms cannot maintain access to a copy of the data within their firm at the headquarters outside of Europe.

Finally, these developments do not only hinder business opportunities in other markets but at the same time risk the loss of international business collaboration that European businesses rely on to offer their own services in the single market: the loss of research collaboration during a global pandemic, the loss of critical national and day-to-day cybersecurity, and the loss of geo-political power from turning inwards and risking retaliation from other regions.

Below we have identified key changes that could be made to the draft Recommendations, and we urge the EDPB to consider these elements and practical implications of the recently published recommendations and revaluate the text accordingly and proportionately.

Executive Summary

AmCham EU makes five key recommendations to improve the EDPB's work on data transfer measures. These are:

- Taking account of the importance of a risk-based approach to data transfers;
- The need to take a proportionate approach to potential risk to data subjects;
- Considering a practical approach to encryption as a protective measure for business use;
- Ensuring coherence with the draft implementing decision on SCCs; and
- Aligning the timeline for the transition and compliance periods with the period foreseen in the European Commission's new SCCs.

Importance of a risk-based approach

Recommendation 1:

Follow a 'risk-based' approach so that businesses can decide on measures based on the risks identified: The EDPB Recommendations should provide a 'risk-based' approach consistent with the GDPR to enable data exporters to assess the law and practice of the importing country taking into account the type of data, the likelihood of access by public authorities and impact on the individual if accessed, and adopt proportionate supplementary measures, commensurate with identified risks.

We recommend to add to §33 that the likelihood of public authorities' access in the specific case of a transfer scenario, as resulting from the evaluation of any relevant contextual element like type of data, nature of the activity and industry category, history of actual surveillance, etc. can complement the other factors for assessing the risk of the transfer. We also ask to clarify §42 to set forth that when legislations in a third country may be lacking, likelihood of access cannot be used as the sole criteria to determine the risk but needs to be factored in the assessment.

In addition, to fully align with a risk-based approach, we recommend that the EDPB requests information from third country data protection authorities (DPAs) or equivalent about the level of adequacy for each of their legal systems and serve as a resource for data exporters who seek greater certainty regarding transfers to certain countries.

Justification

The EDPB's Recommendations 01/2020 on 'supplementary measures' as currently proposed do not seem to effectively implement GDPR's risk-based approach, instead using a concerning one-size-fits-all approach, regardless of the type of data in discussion and the actual likelihood of surveillance being exerted. Instead, the risk-based approach of the Schrems II decision of the CJEU (Judgment in Case C-311/18) and the corresponding fundamental principle enshrined in the GDPR should be adopted. The exporter (assisted by the importer) should be able to factor in all relevant subjective or objective criteria to assess the risk associated with a transfer to a third country on a case-by-case basis. This should include the nature of the data and the likelihood and history of access, interference or a request by a foreign government. Likelihood and precedents based on experience cannot be the only factor, but exporters and importers should be able to predict the realistic risk associated with specific transfers based on prior access requests of public authorities. The likelihood based on the (objective) number of executed access requests by public authorities is a key component of the risk assessment, as the realistic risk of being subject to such a request varies significantly based on the business model of the exporter and importer (data transfers for business purposes vs. social networks), and the data category (business data vs. private information).

§42 states that the assessment in step 3 on whether a transfer tool is effective should not consider 'subjective' factors such as the likelihood of access. While we understand that such a factor may not be central to step 3, it should be a consideration taken into account in identifying appropriate supplementary measures in step 4. In other words, if the data is of limited real-world interest to public authorities, for example business contact

information or other low-risk personal data, it should have a bearing on the type of supplementary measures that are required. The experiences companies have had with these types of requests in the past should also be factored in.

In addition, to ensure alignment with GDPR, the recommendations should stress the risk in terms of impact on the rights and freedoms of the data subjects given the nature of the data and the purpose of the processing, even if they were accessed. The EDPB endorsed Article 29 Working Party's 'Guidelines on DPIAs and determining whether a processing is likely to result in a high risk', according to which data protection impact assessments (DPIAs) are only mandatory when the processing is 'likely to result in a high risk to the rights and freedoms of natural persons, considering the use of new technologies, and taking into account the nature, scope, context and purposes of the processing (Article 35(1) GDPR)'. This risk-based approach is not taken in the EDPB's Recommendations, resulting in a contradictory need for a transfer impact assessment and applying supplementary measures for processing activities that otherwise wouldn't even be subject to a DPIA or deserve such security measures.

Similarly, the new draft SCCs also factor a risk assessment taking into consideration, (i) the specifics of the transfer, eg, the nature of the personal data transferred; (ii) the third country laws including access rights by law enforcement in the third country; and (iii) any additional technical and organisational safeguards (see Clause 2(b)) and not just the third country laws.

Finally, from a practical perspective, the complexity of the assessment process (step 3), which involves analysing and documenting, including on an ongoing basis (step 6), 'if there is anything in the law or practice of the third country that may impinge on the effectiveness of the appropriate safeguards of the transfer tools you are relying on, in the context of your specific transfer', does not scale and will not be workable for companies, especially SMEs, to implement.

Towards a proportionate approach

Recommendation 2:

The EDPB guidance should 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. The flexibility afforded to exporters, in particular, by the GDPR and Schrems II should be respected by the EDPB. Balance should be found in order to graduate measures vis-à-vis risk assessment. The recommendations should also clarify that for all scenarios outlined in the use cases (especially use cases 6 and 7), all risk assessment factors should be available for consideration. For instance, contractual and organisational measures might be considered to sufficiently help to guarantee the protection of personal data transferred in circumstances where the nature of the circumstances (type of data, type of industry, history of surveillance instances) suggests a low risk.

Justification

In the Recommendation 01/2020, organisational and contractual measures are looked at with scepticism and are underlined several times to be insufficient in non-adequate countries if used without technical measures. Primacy is given in the recommendations to the technical supplementary measures. §48 states that contractual and organisational measures will generally not overcome access by public authorities and that there are situations where only technical measures impede access or render it ineffective. Such primacy is risky insofar as it means there is limited incentive as a result to adopt organisational or contractual protections despite their clear value in protecting the data and deterring excessive and disproportionate access.

While contract verbiage does not bind third countries' authorities by nature, any importer's commitment to challenge, redirect or push back against a government request, as well as any transparency measures to inform the exporter/controller of any such request, provide significant protections against government access. Thus,

not only technical, but also a combination of contractual and organisational measures can ensure an essentially equivalent level of protection for data subjects in practice.[1]

A practical approach to encryption

Recommendation 3:

The EDPB Recommendations should consider that the access to industry-standard IT security measures is essential for any business processing data. Technical measures including access to state-of-the art security services should be factored into any case by case risk assessment of transferring data to a third country and consideration of effective technical measures should not be limited to the use of non-decryptable encryption only.

Justification

The recommendations could be interpreted as generally requiring comprehensive encryption at all stages of the data processing, which would result in companies having to implement disproportionate encryption measures, which could be particularly burdensome for SMEs and significantly hamper the ordinary course of business.

A practical example of the consequences of the 'non decryptable encryption' in ordinary business is that it would end up impeding the free accessibility of European originated personnel data even within the same organisation, in case of structures (public and private) organised on a multinational level, with severe impact on the ordinary course of business. For any company headquartered outside of the EU, transferring employee data to HQ is vital for day to day business. Companies should be able to assess performance of employees, compare and set compensation, investigate and resolve employment disputes or complaints, and conduct hiring and termination procedures in a centralised manner. As employee consent is rarely valid under EU data protection law, the recommendation could be read as there would be no valid way to do this after Schrems II judgement. As this would impact thousands of companies, in all sectors across the board, we would recommend reconsidering this issue based on the practical implications and non-tariff trade barriers this would present to all organisations operating in the EU, while headquartered in a third country.

In addition, global cloud service providers offer security services, currently protecting sensitive data from attacks by state-of-the-art protection measures. The EDPB recommendations could incentivise data controllers to prefer less secure service providers that offer entirely local processing. If the recommendations cause companies to prohibit decryption at any point in the processing, IT security could be undermined, as technologies such as packet inspection hinder the transfer of malicious traffic and to absorb distributed denial-of-service (DDoS) attacks. Decryption of the packets is necessary to do this analysis. If this measure is prohibited, many businesses would struggle to maintain a high level of IT security, significantly damaging the resilience and security of IT networks and critical infrastructures. ENISA has specifically highlighted the increasing number of phishing campaigns and ransomware attacks on healthcare systems since the beginning of the COVID-19 crisis.[2] The reality of today's cyber threat landscape means that Europe cannot afford to lower cyber security standards or compromise the resilience of its critical infrastructure by hampering access to security solutions and measures.

Practical implications

The members of AmCham EU have closely read and analysed the impact of the EDPB Recommendations draft and have found that the below practical consequences of their application may not have been taken into consideration:

[1] Cf. also ECJ Judgement, *Schrems II*, Paras. 137, 148.

[2] https://www.enisa.europa.eu/news/enisa-news/cybersecurity-in-the-healthcare-sector-during-covid-19-pandemic

- Multinational companies with employees in and outside the EU: When reading the recommendations (particularly use case #7, page 27, §90-91), they seem to prevent multinational companies (whether based in the EU or outside the EU) with affiliates outside the EU to operate their normal course of business, by suggesting that all EU employees' data can only be transferred in an encrypted way to these non-EU countries and cannot be decrypted there (because use case 7 suggests at the point of decryption, it is an illegal transfer no matter what other strong supplementary contractual and organisational measures are in place). In fact, the outcome of recommendations as they stand now, could even be the cessation of all email exchange between EU affiliates and their third country headquarters.

- SMEs using cloud providers to operate online stores: Smaller companies have greatly increased their participation in international trade transactions using online services based in other jurisdictions to connect with customers and suppliers, provide information, take and place orders, and facilitate the delivery of products and services. The use cases provided for in the EDPB guidance mean that smaller companies that have benefited from greater connectivity with customers and suppliers through online platforms will be seriously impacted if they lose confidence that they can implement sufficient supplementary measures to use these services.

- NGOs and charities using email providers: If international NGOs and charities do not believe they can implement sufficient supplementary measures, they would be precluded from communicating and working on cross-border initiatives using email providers in other jurisdictions. NGOs and charities need to collaborate internationally (including with those in foreign jurisdictions) on day-to-day issues such as to prepare the channels that enable international response, conduct research in their areas and understand global trends.

- Healthcare research initiatives communicating with cloud solutions: Global health care research is necessary in order to advance medicine and collaborate in the field. For example, international collaborations account for almost one-quarter of all publications and international partnerships have been growing between foreign jurisdictions and the EU.

- University research using online collaboration software: EU-based universities engage in collaborative research with institutions and organisations around the world. This research inevitably involves the transfer of personal data to third countries and these organisations need to use online software to communicate and collaborate globally.

- Cloud providers in the EU: Common practices such as using shared systems and providing remote access to data where a parent or group company is based in a foreign jurisdiction may be hindered if businesses are concerned that they cannot use the SCCs. The recommendations would affect all well-known and broadly used cloud service providers that may host data linked to EU nationals outside of the EU. This would result in hindering everyday working life in all organisations, as the use of online meeting platforms provided by non-EU providers would no longer be possible. Such communication tools have become essential for millions of people working from home during the pandemic, as hosting in Europe is simply not an alternative for many of these services. The recommendations would also result in placing barriers to EU-headquartered cloud providers who may have activities or subsidiaries outside of the EU as well, thereby limiting their ability to grow and compete globally.

Coherence with draft implementing decision on SCCs

Recommendation 4:

We recommend that considering the ineliminable intertwining of the SCCs with the EDPB recommendations, the two documents be aligned as much as possible when it comes to their key guiding criteria and implementation and that the risk-based approach is incorporated in both documents.

Justification

The draft decision by the European Commission on SCCs diverge from the recommendations offered by the EDPB, such as in the incorporation of a more a risk-based approach. Taken together §19 and 20 of the new SCCs state that when considering whether the laws applicable to the importer prevent from complying with the clauses, the parties should consider 'any relevant practical experience indicating the existence or absence of prior instances of requests for disclosure from public authorities received by the data importer for the type of data transferred.' This conflicts with the EDPB suggestion not to rely 'on subjective factors such as the likelihood of public authorities' access to your data in a manner not in line with EU standards', although §49 of the EDPB recommendations also suggests the nature of the data transferred should be considered, as well as with the risk-based nature of the GDPR itself.

Considering that the actual SCCs have been used for a decade in thousands of contracts, providing a deep level of protection and safeguard substantially similar to the new SCCs, and that parties are already required to verify if additional measures should be in place following EU Court decision (Case C-311/18), the request to update all the contracts appears not necessary and extremely burdensome. It will still satisfy the aim to secure transfer of data to third countries, if exporter and importer are required to apply them only for the new contracts when the SCCs will come effective. This will also be in line with the Commission instruction of the previous SCCs update. Alternatively, it would be helpful and save a lot of paperwork if the current SCCs would be automatically replaced by the new SCC (taking into account the role of each party), whereby parties will obviously still be required to undertake transfer impact assessments and implement supplementary measures.

Timeline

Recommendation 5:

Align the transition and compliance period with the period included in the Commission's new SCCs, both for consistency and to acknowledge the huge effort required from companies because of complex IT and data ecosystems that operate in today's digital landscape.

Justification

We consider that it is an inconsistent approach to include a transition period to replace the SCCs but to declare the supplementary measures recommendations to be immediately applicable. They are intrinsically linked, with the latter even including a set of contractual recommendations alongside the organisational and technical ones. In addition, it is not clear whether some contractual recommendations are already captured by the new SCCs or whether we need to include additional supplementary clauses in the overall data protection agreement. This needs adequate time to be assessed.

Although the CJEU states in Schrems II that international transfers to countries with an insufficient level of protection should immediately stop, the DPAs should be consistent with the appearance of legitimate confidence that has been created by the fact that they never questioned SCCs as a sufficient mechanism before. In some circumstances, the recommendations will in effect require the complete redesign of the architecture of services, as well as go-to-market supplier, customer contract and organisational changes. We understand that the EDPB Recommendations interpret the CJEU's ruling, which in itself was immediately applicable, and AmCham EU members have been diligently working to ensure that proper safeguards continue to apply to data flows. Nevertheless, we may not achieve perfection immediately, and, as the enforcers of the law, the EDPB has an opportunity to signal its own intentions for an adequate timeline for corrective actions.