www.amcham.ie @americanchamber

AMERICAN CHAMBER of COMMERCE IRELAND

American Chamber of Commerce Ireland submission to the EDPB consultation on Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data

21 December 2020

INTRODUCTION

The American Chamber welcomes the opportunity to provide a submission to the EDPB's public consultation on the recently published 'Recommendations on measures that supplement transfer tools to ensure compliance with the European Union (EU) level of protection of personal data (henceforth the Recommendations)'. We also welcome the extension of the deadline by the EDPB for submissions to the 21st December, noting the importance of allowing adequate time for industry to provide feedback to such important recommendations. It is equally important that time is given to consider the responses from this public consultation, the American Chamber views these Recommendations as the most critical set of Recommendations that the EDPB has adopted to date.

The American Chamber notes that the background to the drafting of the Recommendations stemmed from the CJEU ruling in the Schrems II case which found that organisations that rely on standard contractual clauses (SCCs) to transfer data outside the EU may need to adopt additional safeguards to protect personal data from access by public authorities in third countries. These Recommendations would have provided a useful opportunity for the EDPB to provide data exporters with a 'toolbox' of pragmatic, practical measures that would help them comply with the Court's decision. However, in a number of areas it would appear that the Recommendations do not follow this approach, and the overly prescriptive, non-risk-based approach outlined by the EDPB goes both beyond the requirements of Schrems II outlined by the CJEU and the General Data Protection Regulation (GDPR).

Before providing more detailed points below, the American Chamber underlines the importance of providing certainty for EU businesses and their data transfers to third countries. The American Chamber also highlights the near ubiquitous use of data by organisations, large and small, in every sector in the EU, and that the ability of firms to carry out data transfers cross border are an inherent feature of how firms operate and trade. Any action that stifles or impedes data transfers to third countries outside of the EU would have a profoundly negative impact for businesses, large and small, across the EU.

The American Chamber reiterates our call for the EU to prioritise achieving an agreement with the US to put in place a new mechanism that would replace Privacy Shield, which was invalidated by the CJEU in July 2020. In the short term, noting that a replacement mechanism for Privacy Shield could take some time to negotiate, a short-term political resolution is required between the EU and US. The American Chamber highlights the EU's own ambitions for the EU-US transatlantic relationship, only recently releasing their paper a 'Positive Transatlantic Agenda'[1] and that the EU wishes to 'facilitate free data flow with trust'[2].

[1] '*Joint Communication: A new EU-US agenda for global change*', European Commission, found at https://ec.europa.eu/info/files/joint-communication-new-eu-us-agenda-global-change_en

[2] '*Joint Communication: A new EU-US agenda for global change*', European Commission, p6

A RISK-BASED APPROACH

The EDPB outlines a roadmap that businesses should undertake 'if you (the data exporter) need to put in place supplementary measures to be able to legally transfer data outside the EEA[3].' The roadmap specifically outlines that the data processor must know their transfers, and acknowledges that 'Recording and mapping all transfers can be a complex exercise for entities engaging into multiple, diverse and regular transfers with third countries[4]'. These steps, in and of themselves, are reasonable and in line with obligations under the GDPR.

However, the Recommendations then go on to address different Use Cases where it appears the EDPB has taken an overly narrow, prescriptive and burdensome approach to the analysis of transfers. The Recommendations, when looking at actual scenarios for transfers, appear to focus entirely on a single issue, namely encryption, as opposed to advocating a holistic case by case approach to risk assessment as was advocated for by the CJEU and as is established in the GDPR. This will present an entirely unattainable standard for businesses, and it remains unclear how some businesses, in particular SMEs, would have the capability to implement these measures.

It would be preferable for the EDPB to adopt a more holistic interpretation, rather than a restrictive, absolution interpretation of Schrems II judgement which better reflects the established parameters of EU law under GDPR.

As it stands these Recommendations would place insurmountable obstacles to transfers of personal data outside the EU, rather than following the CJEU in Schrems II to take the full context of the data transfer into account and that data exporters should assess the transfers in the light of all the circumstances of that transfer and on a case-by-case basis. The Recommendations would also require that National Supervisory Authorities, in following the Recommendations, step outside the bounds of existing law under the GDPR, thereby inevitably exposing their decisions to judicial review and creating even greater uncertainty for data controllers.

By way of practical example for the above, the likelihood of National Authorities accessing data, having regard to the categories of data, the nature of the processing, the other technical and organisational measures which are in place, as well as other factors, should be taken into account as part of the full context and risk. However the Recommendations outline that if the data importer falls within the scope

[3] '*Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data*' EDPB, p8
[4] '*Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data*' EDPB, p8

of certain national security laws[5], the data exporter must use additional technical measures irrespective of these other factors. The example outlined in the Recommendations, suggests that these technical measures must be implemented even if the data importer has never received an order to access data for national security purposes or even if the data would be of no relevance.

The American Chamber recommends that the Recommendations align with the risk-based approach of Schrems II and the corresponding fundamental principle enshrined in the GDPR.

The American Chamber notes that this is also the approach taken by the European Commission in their recently published update to standard contractual clauses, and that this risk-based approach is essential to any risk management strategy and business planning of an organisation. It is important that an overly restrictive approach is avoided and a pragmatic approach is instead adopted. It is essential to keep a holistic view 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 American Chamber recommends adding to paragraph 33 that the likelihood of public authorities' access in the specific case of a transfer scenario can complement the other factors for assessing the risk of the transfer, and to clarify paragraph 42 to set forth that, when legislation 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.

CONTRACTUAL AND ORGANISATIONAL MEASURES

The Recommendations state[6] that the use of contractual and organisational measures alone are not sufficient as supplementary measures and that technical measures are essential and the most effective form of supplementary measures. The Schrems II judgment did not suggest that technical measures were more valid, such a position appears to assume that the mere theoretical possibility of access by third-country authorities—even if the practical risk of such access is small—renders a transfer unlawful. However, the American Chamber believes that contractual and organisational measures should not be

[5] '*Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data'* EDPB, p15

[6] '*Contractual and organisational measures alone will generally not overcome access to personal data by public authorities of the third country (where this unjustifiably interferes with the data importer's obligations to ensure essential equivalence). Indeed there will be situations where only technical measures might impede or render ineffective access by public authorities in third countries to personal data, in particular for surveillance purposes'* – paragraph 48, p15, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data'

overlooked and can be effective as supplementary measures when a holistic view and the full context, as outlined above, is taken into consideration.

Likewise, organisational measures such as ISO certifications are also certified mechanisms under GDPR and the global nature of these standards can efficiently help global businesses assess and comply with relevant privacy laws, particularly if the standard is updated to address specific issues such as local surveillance laws.

The American Chamber recommends that the EDPB amend paragraph 48 taking into consideration that a holistic view and a risk assessment can lead to the result that contractual and organizational measures alone can sufficiently protect the data subject. Furthermore, we recommend including a reference to contractual and organizational measures in paragraph 33.

TECHNICAL MEASURES

As outlined above, the Recommendations do not support the view that organisational and contractual measures can effectively be used as supplementary measures, and that technical measures remain the most important tool to protect data transfers. However some of these technical measures, in particular end to end encryption measures would be overly burdensome for business. They are also unworkable in some scenarios such as intercompany arrangements where databases typically require access from around the globe yet the guidance outlines that the key should remain with the exporter. While there is an overall lack of emphasis on risk within the Recommendations, there is a substantial focus on encryption with overly prescriptive recommendations – the American Chamber notes in this context that there are twenty-three references to encryption and only four references to risk within the text itself.

The American Chamber highlights that encryption is just one security measures that can be used and that there are other options available to importer and exporters. For example, if you have a system that has a specific authorisation process, this is as powerful a security tool as encryption. It should be left to the importer and the exporter to decide on the necessary security measure, the reason being that different data will require different levels of security.

By narrowing the consideration of available controls to almost exclusively focus on encryption, the EDPB has disregarded more effective controls. Access control restrictions can prevent technology providers from even accessing data, even if it is processed by systems within secure enclaves. Obfuscation techniques such as masking can ensure data can be safely masked prior to transmission and processing - encryption as described in Use Case 1 is not the only mechanism for masking. Transparent data encryption approaches can effectively create a secure mechanism for a data exporter to expose

unencrypted data on demand to applications only under their control, while the data is maintained in encrypted form to any external party. There are numerous other controls and design approaches that can be applied based on the specific use case and architecture, each of which can provide effective risk mitigations but there is no indication in the opinion that these have been considered.

The Recommendations require that 'the encryption algorithm is flawlessly implemented', this is not aligned with international industry standards when it comes to encryption and the American Chamber recommends aligning with such international standards. The Recommendations should also take into account that access to industry-standard IT security measures is essential for any business processing data. The access to state-of-the art security services must be factored into any risk assessment of transferring data to a third country. **The Recommendations should also clarify that for all scenarios outlined in the use cases (especially use cases 6 and 7), many other factors can be considered.** For instance, contractual and organizational measures should be considered to sufficiently help guaranteeing the protection of personal data transferred.

A requirement to implement end-to-end encryption also raises a technical barrier between firms who have the engineering capacity to build this solution, and smaller firms who lack the resources to implement it and are thus excluded from data transfers. It is not practical that an SME would have the resources to hire or even manage a security team to meet these requirements, this is the practical impact of a non a risk-based approach. The American Chamber highlights the reference to the specific needs of micro, small and medium sized enterprises within GDPR[7].

ENFORCEMENT & COMPLIANCE

The Court's holding in Schrems II was a major and unexpected development, one that is requiring organisations across the EU to prepare new data transfer impact assessments and, in certain cases, to overhaul aspects of their data transfers. In many cases, these efforts require changes not only to contracts, but also to underlying infrastructure, software, and systems. Undertaking these changes is a complex task that often will involve many different parties, both inside and outside an organisation. Notwithstanding these facts, the Recommendations imply that supervisory authorities should move directly to 'corrective measure[s] (e.g. a fine)'[8] if they determine that a data transfer does not comply

[7] Recital 13 of the GDPR : In addition, the Union institutions and bodies, and Member States and their supervisory authorities, are encouraged to take account of the specific needs of micro, small and medium-sized enterprises in the application of this Regulation. The notion of micro, small and medium-sized enterprises should draw from Article 2 of the Annex to Commission Recommendation 2003/361/EC.

[8] '*Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data'* EDPB, p17

with the Recommendations. This focus on sanctions will lead EU organisations to rush through changes to their data transfer practices—making it far less likely that organisations address these issues carefully and precisely. To avoid this outcome, **the Recommendations should expressly advise supervisory authorities, when they determine that a specific data transfer does not comply with EU law, to work with data exporters to find acceptable safeguards, and give them sufficient time to implement such solutions.** This approach will provide incentives for EU organisations to address these issues thoughtfully, while also encouraging good-faith, collaborative solutions to these quite difficult legal and technical issues.

Furthermore, in paragraphs 10, 31 and 33, the EDPB refers to the necessity to consider 'all actors participating in the transfer'. This means that the exporter, assisted by importer, would be required to list the full chain of sub-processors potentially in an infinite way, which in practice, in complex supply chains is close to unfeasible. Likewise, obligating importers to ensure that sub-processors comply with data importer obligations sets an unachievable standard. **The American Chamber recommends that it should be sufficient that the data importer is responsible for the performance of the sub processor obligations.**

STEP 5 OF THE RECOMMENDATIONS

The American Chamber notes 'Step 5- Procedural steps if you have identified effective supplementary measures' that are outlined within the Recommendations. This step outlines an obligation to consult the relevant DPA[9], for example, where you intend to modify the standard data protection clauses. The American Chamber highlights the wider impact of this including the level of resourcing that would be required within the relevant authorities.

[9] 'Where you intend to modify the standard data protection clauses themselves or where the supplementary measures added 'contradict' directly or indirectly the SCCs, you are no longer deemed to be relying on standard contractual clauses and must seek an authorisation with the competent supervisory authority in accordance with Article 46(3)(a) GDPR' p17 of the Recommendations

ANNEX: AMERICAN CHAMBER SUMMARY OF RECOMMENDATIONS

- The American Chamber recommends that EDPB adopt a more holistic interpretation, rather than a restrictive, absolution interpretation of Schrems II judgement which better reflects the established parameters of EU law under GDPR.

- The American Chamber recommends that the Recommendations align with the risk-based approach of the Schrems II and the corresponding fundamental principle enshrined in the GDPR.

- The American Chamber recommends adding to paragraph 33 that the likelihood of public authorities' access in the specific case of a transfer scenario can complement the other factors for assessing the risk of the transfer, and to clarify paragraph 42 to set forth that, when legislations in 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.

- The American Chamber recommends that the EDPB amend paragraph 48 taking into consideration that a holistic view and a risk assessment can lead to the result that contractual and organizational measures alone can sufficiently protect the data subject. Furthermore, we recommend including a reference to contractual and organizational measures in paragraph 33.

- The Recommendations require that 'the encryption algorithm is flawlessly implemented', this is not aligned with international industry standards when it comes to encryption and the American Chamber recommends aligning with such international standards.

- The Recommendations should also clarify that for all scenarios outlined in the use cases (especially use cases 6 and 7), many other factors can be considered.

- The Recommendations should expressly advise supervisory authorities, when they determine that a specific data transfer does not comply with EU law, to work with data exporters to find acceptable safeguards, and give them sufficient time to implement such solutions.

- The American Chamber recommends that it should be sufficient that the data importer is responsible for the performance of the sub processor obligations.

- The American Chamber highlights the wider impact of this including the level of resourcing that would be required within the relevant authorities.