AFME and SIFMA joint comments to the EDPB's measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data

December 10, 2020

VIA PUBLIC CONSULTATION REPLY FORM

The Association for Financial Markets in Europe[1] ("AFME") and the Securities Industry and Financial Markets Association ("SIFMA")[2] welcome the opportunity to comment on the version of the Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (the "Recommendations") published by the European Data Protection Board (the "EDPB") on November 11, 2020,[3] as input for the final Recommendations.[4]

Further to the judgment of the Court of Justice of the European Union (the "CJEU") handed down on July 16, 2020, in *Data Protection Commissioner v. Facebook Ireland and Maximillian Schrems* ("*Schrems II*"), the EDPB was essentially expected to provide clarity on:

- the criteria which data exporters should use to assess whether the laws of a particular third country enable data importers located there to comply with standard contractual clauses ("SCCs"); and
- what additional safeguards could be put in place by data exporters and importers in order to remedy any issue identified when making that assessment.

[1] AFME represents a broad array of European and global participants in the wholesale financial markets. Its members comprise pan-EU and global banks as well as key regional banks, brokers, law firms, investors and other financial market participants. We advocate stable, competitive, sustainable European financial markets that support economic growth and benefit society. AFME is the European member of the Global Financial Markets Association ("GFMA"), a global alliance with SIFMA in the United States, and the Asia Securities Industry and Financial Markets Association ("ASIFMA") in Asia. AFME is registered on the EU Transparency Register, registration number 65110063986-76.

[2] SIFMA is the leading trade association for broker-dealers, investment banks and asset managers operating in the U.S. and global capital markets. On behalf of our industry's nearly 1 million employees, we advocate for legislation, regulation and business policy, affecting retail and institutional investors, equity and fixed income markets and related products and services. We serve as an industry coordinating body to promote fair and orderly markets, informed regulatory compliance, and efficient market operations and resiliency. We also provide a forum for industry policy and professional development. SIFMA, with offices in New York and Washington, D.C., is the U.S. regional member of GFMA, a global alliance with AFME in Europe and ASIFMA in Asia.

[3] https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf.

[4] AFME and SIFMA wish to thank Emmanuel Ronco and Natalie Farmer of Cleary Gottlieb for their assistance in preparing this response.

Association for Financial Markets in Europe
London 39th Floor, 25 Canada Square, London E14 5LQ, United Kingdom T: +44 (0)20 3828 2700
Brussels Rue de la Loi 82, 1040 Brussels, Belgium T: +32 (0)2 788 3971
Frankfurt Bürohaus an der Alten Oper, Neue Mainzer Straße 75, 60311 Frankfurt am Main, Germany T: +49 (0)69 153 258 967
www.afme.eu

Securities Industry and Financial Market Association
New York 120 Broadway, 35th Floor | New York, NY 10271
Washington 1099 New York Avenue, NW, 6th Floor | Washington, DC 20001
www.sifma.org

We appreciate the EDPB's efforts to streamline the process of selecting the right transfer tool and, where required, implement appropriate supplementary measures using a step-by-step roadmap. However, AFME's and SIFMA's members remain generally concerned that the Recommendations, in their current form, would not solve the risks of inconsistency among both, data exporters and supervisory authorities, thereby generating a lack of visibility and certainty for data subjects and placing an undue burden on data exporters and importers wishing to engage in data transfers that are vital to their businesses. In addition, the Recommendations should be aligned with the revised SCCs that are in the process of being adopted by the European Commission, a draft of which was issued for public consultation the day after the Recommendations (the "New SCCs").[5]

Our comments below intend to provide constructive suggestions to attempt to reconcile the interests of data exporters, importers and data subjects while complying with the standards set out in *Schrems II* and the General Data Protection Regulation (the "GDPR").

Executive Summary

AFME and SIFMA urge the EDPB to consider the following when preparing the final version of the Recommendations:

1. ***Establish a resource centre on the "law and practice" of third countries and provide a template for their assessment***. The requirement to undertake a case-by-case analysis of the legal systems of third countries will inevitably give rise to uncertainty and inconsistency; given that multiple data exporters will be undertaking such assessments in parallel, this creates a multiplication of costs which are in any event individually burdensome. A consistent and efficient appraisal of third countries' data protection laws and practices would be greatly facilitated by (i) establishing (possibly with other institutions) a resource centre where updated legislative sources as well as pertinent case law and commentaries on the privacy and surveillance laws of third countries would be available to enable an equal access to information for all data exporters in the EU and which data exporters may supplement with their own research, and (ii) providing an indicative template for assessing the law and practice of third countries with different assumptions (which can be used as a precedent for similar analyses by data exporters).

2. ***Follow a "risk-based" approach enabling exporters to determine which measures should be used depending on identified risks to individuals***. The Recommendations provide illustrations of proposed supplementary measures based on "Use Cases" with strict assumptions,

[5] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12741.

which do not give sufficient leeway to data exporters to handle the majority of situations which are often more complex. Instead, the Recommendations should offer a "risk-based" approach consistent with the GDPR to enable data exporters to (i) assess the law and practice of the recipient country taking into account the circumstances of the transfer, including the nature of the data and the likelihood of access by public authorities in the recipient country, (ii) establish a "sliding scale" of risk levels and adopt proportionate supplementary measures, which may or may not include technical measures, commensurate with identified risks, and (iii) rely on precedent analyses for similar transfers, subject to regular updates.

3. ***Avoid the suggestion that cloud computing and remote access to data in the clear are always prohibited***. The Use Cases concerning cloud computing and remote access to data in the clear may be read as closing all avenues for data exporters to give effect to such transfers, which are critical to EU businesses. Instead, the Recommendations should also allow data exporters to use a risk-based approach to come to their own conclusion (having regard to the nature of the data and risks of access by public authorities) and consider either that no supplementary measure would be sufficient, or that a combination of technical measures, such as pseudonymisation in tandem with contractual and organisational measures for instance, could be put in place to permit the transfer.

4. ***When possible, enable data exporters to conduct a risk assessment for "in transit" data***. The Recommendations suggest that, when the transferred data will transit through third countries before reaching their final destination, they will be required to be encrypted during transport or, if needed, even end-to-end. This is presumably based on the default assumption that the data exporter will not know the countries in which the data will be in transit. However, if data transit through identified countries, the Recommendations should enable data exporters not to encrypt "in transit" data if their risk assessment leads them to adopt no, or less stringent, supplementary measures.

5. ***Clarify that each onward transfer is to be assessed by the person effecting that transfer***. It may be impossible (and in any event, highly burdensome) for a data exporter to assess all potential onward transfers effected by the data importer. The initial data exporter may not control, or even be aware of, all onward transfers (i.e., further transfers of the data by the data importer and any other onward transferee). The responsibility of the initial exporter regarding onward transfers should be limited to requiring that the data importer (i) carry out the assessment and use supplementary measures based on the steps laid out by the Recommendations, but not to make

that assessment itself and (ii) impose the same obligations on follow-on data transferors to ensure the protection of the data down the chain.

6. ***Set appropriate encryption standards***. Encryption appears to be the preferred supplementary measure set out by the Recommendations. However, for encryption to be deemed effective, the Recommendations require excessively high standards set out in the assumptions of the Use Cases concerning encryption, including the flawless implementation of the encryption algorithm or the retention of the encryption keys solely by the data exporter in certain cases. These standards would neither enable nor encourage the use of encryption by many data exporters and importers. Instead, the Recommendations should require the use of "appropriate" encryption standards (based on the GDPR's requirement for appropriate technical and organisational measures) that are proportionate with the cryptanalysis resources of the recipient country and allow non-exclusive control of encryption keys, at least when identified risks of access are low.

7. ***Set appropriate pseudonymisation standards***. The Use Case concerning the transfer of pseudonymised data assumes that the additional information required to re-identify the data subjects is held "exclusively by the data exporter." This does not seem to be required for that measure to be effective, as long as that additional information is not available to the data importer.

8. ***Clarify that technical measures are not intended to block all data access requests by third countries***. The Recommendations suggest that there are situations in which only technical (as opposed to contractual or organisational) measures may create an obstacle to "attempts from public authorities to access data." However, technical measures, such as encryption, should be used to prevent public authorities in recipient countries from accessing the transferred data without authorisation from the data controller or prior notification to the data importer, but not as a way to block all governmental requests to access data (e.g., through a subpoena). In the event that such request is made by a public authority in a third country, it should be up to the data controller to assess whether the provision of the data is compatible with the conditions set out in the GDPR.

9. ***Remove the recommendation to obtain the data subject's consent in the event of a data access request by third countries***. The Recommendations suggest that the parties to the transfer of data in plain text in the normal course of business should agree to request the express or implied consent of the data subject when the data importer receives a requests to access data by a third country's public authority. That step would appear unnecessary as (i) such consent may not be valid under the GDPR (as the Recommendations themselves recognise) or even

obtainable in practice, and (ii) valid consent of the data subject would allow the transfer of data based on a GDPR derogation without resorting to the transfer tools that are the object of the Recommendations.

10. ***Align the Recommendations with the New SCCs***. The EDPB should coordinate with the European Commission to ensure consistency of the Recommendations with the approach reflected in the New SCCs, including with respect to onward transfers, factors to take into account when assessing third countries' laws and practices and the supplementary contractual measures set out in the Recommendations that are already included in the New SCCs.

* * *

1. Establish a Resource Centre on the "Law and Practice" of Third Countries and Provide a Template for their Assessment

The Recommendations state that it is the "primary responsibility of exporters to ensure that the data transferred is afforded a level of protection essentially equivalent to that guaranteed within the EU"[6] by reviewing publically available legislation. Where the legislation is "lacking", the data exporter then has to consider other relevant and objective factors. However, the current version of the Recommendations do not provide more than high-level principles and sources of information with respect to the assessment of the data protection "law and practice" of third countries as described in Step 3.

This approach would leave data exporters in almost the same situation as they were before the Recommendations were issued, as they would continue to be faced with:

- a challenging and risky analysis (in particular having regard to the possible sanctions if the assessment is later deemed to be incorrect and, perhaps even more importantly, the perspective that data transfers may have to be stopped or transferred data repatriated);
- an onerous and time-consuming assessment that would prevent any urgent transfer of data and that would have a serious impact on the risk-benefit analysis of transfers that were until now commonplace or necessary (in particular at a time when remote working and e-commerce are becoming the norm);

[6] Recital (8) of the Recommendations.

- an imbalance between large companies with sophisticated advisors and small and medium enterprises that may not have the resources necessary to conduct such assessment; and

- uncertainty when the laws of third countries are difficult to access or understand, in which case many exporters would choose to abstain from transferring data to such countries, which may therefore be penalised and deprived of data-dependent business from the EEA, despite potentially meeting the conditions for importing personal data.

More generally, in the absence of additional guidance on the law and practice of third countries, both exporters and supervisory authorities may come to divergent conclusions with respect to the law and practice of the same country. The Recommendations in their current form therefore do not solve the risk of inconsistency that was highlighted by the CJEU itself in *Schrems II*,[7] leaving exporters and importers, and, more importantly, the data subjects with no visibility as to where the data may be transferred and under what conditions. This is also a costly and onerous analysis which will need to be conducted by multiple data exporters in parallel. As well as creating uncertainty and inconsistency, this will also result in an unnecessary multiplication of costs for EU data exporters.

We therefore urge the EDPB to consider:

- without prejudice to data exporters and importers conducting their own research, establishing (potentially in collaboration with other institutions) a resource centre maintaining a continuously-updated database setting out, in their original version and/or in at least one EU language if necessary, the relevant legislation, case law and pertinent available commentaries describing the law and practice of third countries, in particular those which would otherwise be almost impossible to access for many small or medium enterprises; and

- providing an indicative template for the assessment of the law and practice of a third country, based on various hypotheses for different legal systems (rather than on the current laws and practices of an actual third country which are subject to change), that would serve as a precedent for similar analyses are to be conducted by data exporters.

[7] "As regards the fact, underlined by the Commissioner, that transfers of personal data to such a third country may result in the supervisory authorities in the various Member States adopting divergent decisions, it should be added that, as is clear from Article 55(1) and Article 57(1)(a) of the GDPR, the task of enforcing that regulation is conferred, in principle, on each supervisory authority on the territory of its own Member State. Furthermore, in order to avoid divergent decisions, Article 64(2) of the GDPR provides for the possibility for a supervisory authority which considers that transfers of data to a third country must, in general, be prohibited, to refer the matter to the European Data Protection Board (EDPB) for an opinion, which may, under Article 65(1)(c) of the GDPR, adopt a binding decision, in particular where a supervisory authority does not follow the opinion issued." (*Schrems II*, §147).

2. Follow a Risk-Based Approach Consistent with the GDPR

The Recommendations state that:

- a third country's data protection regime should be assessed not only with respect to its law but also to its "practice"[8] – this implies that extra-legal criteria should be taken into consideration when assessing whether the public authorities of that country do, in practice, access personal data; and

- the "applicable legal context will depend *on the circumstances of the transfer*", including the "categories of personal data transferred."[9] The data exporter is indeed not required to carry out a general adequacy analysis of the laws of a third country similar to that of the European Commission when taking an adequacy decision pursuant to article 45 of the GDPR. Instead, the data exporter should conduct its assessment of the law and practice of a given third country only with a contemplated transfer in mind. This is also consistent with the ruling in *Schrems II* that supervisory authorities have to assess the lawfulness of each transfer "in the light of all the circumstances of that transfer."[10]

When read together, the foregoing would logically imply that data exporters should conduct an analysis of the relevant guidance, statements from public authorities or experience of local professionals on how rules are actually interpreted (i.e., a country's "practice") and also take into account the nature of the transferred data, their interest to public authorities and such public authorities' practice in accessing them (i.e., the circumstances of the transfer). Yet, the Recommendations discourage looking at whether it is "likely" that the transferred data will in practice be accessed by public authorities, dismissing this consideration as "subjective".[11]

The reference to a country's "practice" should be viewed holistically, and not only negatively,[12] when assessing whether a third country offers a substantially equivalent level of protection as that of the EU. In the present case, the risk to individuals will only materialise when the public authorities of the third country actually access the data to be transferred. The likelihood of that risk in the context of the

[8] §29, §30, §43, §44, §60, §66, §107 and §108 of the Recommendations.

[9] §33 of the Recommendations.

[10] *Schrems II*, ruling 3.

[11] §42 of the Recommendations.

[12] §43 of the Recommendations suggests that the "practice" of third countries, as set out in non-legislative sources, may only be considered to complete an initial assessment with "elements demonstrating that a third country authority will seek to access the data with or without the data importer's knowledge."

contemplated transfer is therefore a key factor in assessing a country's actual data protection practice since possible supplementary measures will need to be adapted to the risk identified in making that assessment.

Whether a risk is "likely" is a criterion that is used throughout the GDPR itself and should not be automatically viewed as "subjective". For instance:

- the responsibility and liability of the controller for any processing depends on its implementation of appropriate and effective measures, which are to be determined based, in part, on the likelihood of the risk to the data subject;[13]
- data protection impact assessments are to be conducted when processing operations are likely to result in a high risk to the rights and freedoms of natural persons;[14] and
- notification of a personal data breach does not have to be made to supervisory authorities if it is unlikely to result in a risk to the rights and freedoms of natural persons[15] and is required to be made to the data subjects only if it is likely to result in a high risk to them.[16]

More importantly, the GDPR provides that technical and organisational measures to be implemented by the controller must be assessed based on, *inter alia*, the *likelihood of risks* for the rights and freedoms of natural persons. In the present case, supplementary measures that are the object of the Recommendations fall in the scope of technical and organisational measures and it would therefore only be natural that they be assessed in accordance with the criteria set out in the GDPR itself. The Recommendations themselves provide that the "nature of the data" should be taken into account when assessing the effectiveness of proposed supplementary measures.[17] The "risks involved in the processing" and the "nature of the personal data" to be transferred are also material factors to take into account in "assessing the appropriate level of security" according to the New SCCs.[18]

Given the fact that supplementary measures to be adopted in accordance with Step 4 will need to be tailored to the law and practice of the recipient country to be assessed in Step 3, it would therefore be

[13] Article 24 and recitals (74) to (77) of the GDPR.

[14] Article 35 and recitals (75), (84) and (89) to (93) of the GDPR.

[15] Article 33 and Recital (85) of the GDPR.

[16] Article 34 and recital (86) of the GDPR.

[17] §49 of the Recommendations.

[18] Clause 1.5(a) (Module One), clause 1.6 (Module Two and Three) and clause 1.2 (Module Four) of the New SCCs.

essential to enable data exporters to take into account whether access to the transferred data by that country's public authorities is "likely". This assessment will need to be made in consideration of, among other factors, the nature of the data to be transferred and whether public authorities have, in prior instances, accessed such data and in what circumstances.

This is the approach retained by the New SCCs, which include a warranty that the parties "*have no reason to believe* that the laws in the third country of destination (…) prevent the data importer from fulfilling its obligations under these Clauses" based on an "understanding that laws that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one the objectives listed in Article 23(1) GDPR, are not in contradiction with the Clauses." In giving that warranty, the New SCCs provide that the parties are to take into account, *inter alia*: "the *specific circumstances of the transfer*, including the content and duration of the contract; the scale and regularity of transfers; the length of the processing chain, the number of actors involved and the transmission channels used; the type of recipient; the purpose of processing; *the nature of the personal data transferred*; any *relevant practical experience with prior instances, or the absence of requests for disclosure from public authorities received by the data importer for the type of data transferred*."[19]

A risk-based approach would also enable the data exporter to determine whether a combination of contractual and organisational measures may sometime be sufficient to mitigate the risks of the transfer to the individual, in particular where access to data by public authorities in the recipient country appears highly unlikely. This would be impossible under the current version of the Recommendations, which suggests that contractual and organisational measures may never be sufficient on their own without technical measures,[20] which appear to be essentially limited to strong encryption and pseudonymisation. This would result in unwarranted and significant business disruptions as these measures may be inadequate for the intended use of transferred data even when the likelihood of them being accessed by public authorities would be remote. This may also cause exporters to rely more extensively on derogations set out in article 49 of the GDPR, which would be contrary to the intent of the EDPB even could ultimately be less protective for data subjects.

Finally, by analogy with data protection impact assessments,[21] there may be circumstances under which a properly documented assessment of a country's law and practice made for a particular transfer may be

[19] Clause 2(b)(i) of the New SCCs (all Modules).

[20] §48 of the Recommendations.

[21] Article 35(10) and recital (92) of the GDPR.

used more broadly for additional similar transfers (e.g., in terms of nature of the personal data, purposes and means of the transfer and categories of recipients) to the same country. In that case, to avoid uselessly repeating an onerous and time-consuming process, it should be clear that a data exporter may be allowed to rely on it in the future for similar transfers to the same country provided that it has verified that no changes in the law or practice of that country would warrant conducting another assessment.

The Recommendations should therefore enable data exporters[22] to:

- take into account whether it is likely that the transferred data will, in practice, be accessed by the public authorities of that country, having regard to the circumstances of the transfer, including the nature of the data contemplated to be transferred in conjunction with the country's practice in that regard;
- use a "sliding scale" of risk levels to determine whether strong technical measures are required (when the risk level is high) or contractual and/or organisational measures may suffice on their own (without a requirement to use technical measures such as encryption), for instance when access to the transferred data is highly unlikely based on the practice of the recipient country; and
- once an assessment has been made and documented for a transfer to a given third country, rely on it as a precedent for further similar transfers to that country provided that the assessment is updated in the event of a change in the law and practice of that country.

3. Avoid Apparent "*Per Se*" Prohibitions of Cloud Computing or Remote Access to Data in the Clear

Many will interpret the fact that EDPB states that it is "incapable of envisioning an effective technical measure" applicable in the cases of cloud services requiring access to data in the clear (Use Case 6) and remote access for business purposes (Use Case 7)[23] as "*per se*" prohibitions of these data transfers. However, that interpretation would seem incompatible with the underlying principle set out in the Recommendations that it is the primary responsibility of data exporters make the assessments described in the various steps of the Recommendations.[24] Exporters should therefore be free to mitigate the risks of data transfers in the scenarios described in these two Use Cases by using supplementary measures, including, but not limited to, those described in the Recommendations.

[22] Data exporters includes for this purpose any person affecting a transfer, including onward transfers (as further described in item 5, below).

[23] §88 and §90 of the Recommendations.

[24] Recital (8) of the Recommendations.

The disruption caused by a sudden suspension of all cloud-based or remote-access transfers of data in the clear would also have disproportionate consequences on EU businesses and individuals, as well as possible detrimental effects on the overall level of data security in the European Union. Reliance on cloud computing and remote access has become so commonplace, in particular in the past months as a reaction to the COVID-19 pandemic and the widespread practice of remote working, that an outright ban of these practices would have a potentially disastrous impact on EU-based businesses and, ultimately, European consumers and employees. Storing data using a professional cloud service provider has also often been proven to offer stronger security assurances than storing them in a local server, even if it is located in the European Union. The Recommendations may therefore have unintended adverse impacts on EU data security.

Use Cases 6 and 7 also appear to be framed as alternatives between keeping "data in the clear" (in which case the transfers would be prohibited) and encrypted data (in which case there would be a chance that the transfers would be permitted in accordance with Use Cases 1 and 3). Encryption would make the data unintelligible and therefore unusable by the recipient. Pseudonymisation should not be overlooked as an alternative technical measure which offers a strong level of protection if the data is accessed without authorisation while not depriving it of utility, as data may still be processed even if it cannot be attributed to a specific data subject. Pseudonymisation is also explicitly mentioned as a possible additional security measure to be considered in the "security of processing" clauses of the New SCCs[25] and in the GDPR as a data minimisation measure,[26] and helping making data breaches "unlikely to result in a risk to the rights and freedoms of natural persons,"[27] which is the fundamental objective of supplementary measures. There are also situations in which pseudonymisation may not be appropriate in light of the purpose of the processing, in which case other types of measures should be able to be considered by the data exporter based on the nature of the data and identified risks of access by public authorities in the recipient country.

The EDPB should therefore consider specifying that, while effective supplementary measures may be challenging to implement in the situations described in Use Cases 6 and 7:

- the data exporter may still assess, in collaboration with the data importer, whether a combination of other appropriate contractual, technical or organisational measures (including, but not limited to pseudonymisation) may enable the transfer to meet the substantial equivalence standard, taking

[25] Clause 1.5(a) (Module One), clause 1.6 (Module Two and Three) and clause 1.2 (Module Four) of the New SCCs.

[26] Article 25 of the GDPR.

[27] Articles 32 to 34 of the GDPR.

into account other factors, including the nature of the data, the likelihood of access and harm to data subjects; and

- future technological development may also benefit the assessment for remote access transfers for business purposes described in Use Case 7 (and not only Use Case 6 as is currently the case).

4. When Possible, Enable a Risk Assessment for "In Transit" Data

Use Case 3 suggests that, when transferring data over the Internet such that it "may be geographically routed" through a third country not providing an essentially equivalent level of protection before it reaches the recipient country, the exporter should implement the specific technical measures described in that Use Case (transport encryption, if needed in combination with end-to-end content encryption).[28] This appears to be a default position to be taken even when the third countries through which the data will transit are not identified and the step-by-step analysis described in the Recommendations cannot be conducted.

The EDPB should consider clarifying that if a third country through which the data transits may be identified, the data exporter may also implement no supplementary measure or rely on other types of supplementary measures, after making an assessment in accordance with Step 3 and Step 4.

5. Clarify Obligations Concerning Onward Transfers

Both Step 1 and Step 3 of the Recommendations provide that onward transfers (i.e., transfers made by the data importer and onward recipients of the data) fall in the scope of the Recommendations. However, the initial data exporter cannot be held liable for all onward transfers and the Recommendations should clarify that the obligations to identify onward transfers (Step 1) and assess the effectiveness of the transfer tools for onward transfers (Step 3) do not apply to the initial exporter but rather to the data importer (and others down the chain) conducting such onward transfers.[29]

Indeed, it may be impossible (and in any event, highly burdensome) for a data exporter to assess all potential onward transfers effected by the data importer. The initial exporter may not have knowledge of all onward transfers. The person conducting the onward transfer is therefore best placed to complete both Step 1 and Step 3, as it will be implementing the transfer tool (e.g., by entering into new SCCs with the onward data importer) or ensuring that other grounds for transfer apply as described in the

[28] §84 of the Recommendations.

[29] With respect to the nature of this assessment, a "risk-based" approach should be permitted (as described in item 2 above).

Recommendations, as well as choosing and performing any supplementary measures necessary to achieve an essentially equivalent level of data protection, and will bear the responsibilities in that regard. This would not only be the most pragmatic position, it would also be consistent with the definition of "You" in the Recommendations, which designates the controller or processor acting as data exporter in the contemplated transfer.[30]

This approach appears to be reflected in the New SCCs, in which the data importer (acting as onward data exporter) bears the responsibility of carrying out onward transfers only if they meet certain conditions, including by causing the third party to ensure "appropriate safeguards pursuant to articles 46 or 47 of the GDPR", or, when the data importer is a controller, obtaining the third party's agreement to be bound by the original SCCs, entering into an agreement with the third party ensuring the same level of data protection as under the SCCs or obtaining the explicit consent of the data subject.[31]

This clarification is not intended to detract the responsibility of the initial data exporter, which, when using transfer tools of a contractual nature such as SCCs, *ad hoc* contractual provisions or binding corporate rules, would still have the obligation to bind the data importer to carry out the assessment set out in the Recommendations and implement supplementary measures when necessary if it intends to carry out any onward transfer. The same obligations would therefore apply to any future onward data exporter to ensure consistency in the level of data protection down the chain.

6. Set Appropriate Encryption Standards

The two Use Cases set out in Annex 2 of the Recommendations involving encryption (Use Case 1 and Use Case 3)[32] assume, as a condition to effectiveness of the technical measure, that:

- encryption can be considered robust against cryptanalysis by public authorities in the recipient country;

[30] §6 of the Recommendations provides: "What follows is a roadmap of the steps to take in order to find out if you (the data exporter) need to put in place supplementary measures to be able to legally transfer data outside the EEA. "You" in this document means the controller or processor *acting as data exporter*, processing personal data within the scope of application of the GDPR – including processing by private entities and public bodies when transferring data to private bodies."

[31] Conditions for onward transfers are set out in Section II, Clause 1.7 (Module One) and Clause 1.8 (Modules Two and Three) of the New SCCs.

[32] §79 and 83 of the Recommendations.

- the encryption algorithm will be “flawlessly implemented”; and
- encryption keys should be “retained solely under the control of” (Use Case 1) or “reliably managed by” (Use Case 3) the data exporter or an entity entrusted with this task in the European Economic Area or a country which has been granted an adequacy decision by the European Commission.

Encryption appears to be the technical measure that is most widely recommended in the Recommendations. It is therefore important that the encryption standards set by the Recommendations be strong but not so high as to be impracticable, unachievable or excessively onerous, which would have the unintended consequence of discouraging data exporters from using them.

Cryptography is usually implemented in a hierarchical manner, which involves decentralised and non-exclusive control of keys to mitigate risks associated with external threats, potential outages and to ensure operational resiliency. In addition, multinational organisations often do not segregate data on a jurisdictional basis, due to the use of shared applications, shared infrastructure and due to necessary intragroup data sharing requirements for legitimate business purposes (including risk management and to satisfy legal or regulatory obligations). The Recommendations would potentially require application and infrastructure redesign, segregation and relocation of support teams and business processes, similar to UK ring fencing of wholesale and retail businesses, which took several years and involved significant costs.

Finally, there are situations in which, regardless of where the encryption keys are stored, the data will need to be decryptable at their destination, including for the purpose of assessing operational resilience.

As a result, the EDPB should consider:

- specifying that an assessment of the robustness of encryption measures against cryptanalysis by public authorities may vary depending on the country and through time;
- use an “appropriateness” standard having regard to the state of the art rather than a “flawlessly implemented” standard, consistent with the standard applicable to safeguards to transfer personal data to third countries pursuant to article 46 of the GDPR and technical and organisational measures to be put in place to ensure the security of processing pursuant to article 32 of the GDPR; and
- use only the “reliably managed” standard (and not the “sole control” standard) with respect to encryption keys in Use Case 1 (as is the case in Use Case 3). If the “sole control” criterion is

nevertheless retained, the EDPB should clarify that the data exporter may control the encryption keys either operationally or contractually through an agreement with a service provider in charge of managing them. The EDPB may also then clarify that the lack of "sole control" of encryption keys may be outweighed by contractual or organisational measures, in particular when sole control would be disproportionate having regard to the nature of the data and likelihood that public authorities would access them in the recipient country.

7. Set Appropriate Pseudonymisation Standards

Use Case 2 suggests that, for pseudonymisation to be considered as an effective supplementary measure, the additional information necessary for the data to be attributable to a specific data subject (the "Additional Information") should be "held exclusively by the data exporter" and "kept separately" in the EU or in a third country having been granted an adequacy decision by the European Commission.

However, there are circumstances in which exclusive control of the Additional Information by the data exporter may be neither feasible nor desirable. The Additional Information may not be in the hands of the data exporter, which could have received the data in pseudonymised form to begin with, in particular in the case of transfers in which the data exporter is a processor acting on behalf of a controller which may be in the possession of the Additional Information. Furthermore, as provided for in Use Case 5, the data could be subject to split or multi-party processing (in connection with which two or more data importers could be in possession of Additional Information, vis-à-vis the data set being processed by the other). The New SCCs appear to recognise this as they qualify the clause relating to the control of the Additional Information by the data exporter by "where possible".[33]

The appropriate level of protection required for pseudonymisation to be considered an effective supplementary measure should therefore only be that the Additional Information not be communicated or accessible to the data importer.

The Recommendations should therefore recognise that pseudonymisation is effective so long as the data importer cannot access the Additional Information, irrespective of the identity of the party that is in control of the Additional Information or its location.

8. Clarify that Technical Measures Are Not Intended to Block Data Requests by Third Countries

[33] Clause 1.6 of Section II (Modules Two and Three) of the New SCCs.

The Recommendations provide in Step 4 that "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" and that supplementary measures may strengthen the level of data protection by "creating obstacles for attempts from public authorities to access data."[34]

The foregoing should only apply when public authorities attempt to access transferred data covertly without any notice or request to the data importer. In that case, "appropriate technical and organisational measures" would, in any event, have to be implemented pursuant to article 32 of the GDPR to prevent unauthorised access.

However, if a country's public authority makes a request to the data importer to be provided with specific data, the EDPB should consider clarifying that the parties do not have an obligation to block access to such data by implementing the technical measures set out in the Recommendations such as encryption. In that case, an analysis of the request would have to be conducted to assess whether there is a ground for providing the data in accordance with the GDPR and, when this is not the case, contractual measures can be put in place to ensure that such requests will be contested by the parties.

9. Data Subject Consent When Data Importer Receives Requests from Public Authorities

The Recommendations provide that the parties to SCCs or *ad hoc* contractual clauses could agree to provide that personal data transmitted in plain text in the normal course of business may only be accessed "with the express or implied consent of the exporter and/or the data subject."[35] They further specify that the data subject may not always be in a position "to give a consent that meets all the conditions set out" in the GDPR, citing the case of employees.[36]

The utility of seeking the data subject's consent in that situation is unclear. On the one hand, if the explicit consent of the data subject can been validly obtained, there would be no need for supplementary measures to the SCCs or the ad hoc contractual clauses, as the transfer of the data to the public authorities may be based on a derogation under article 49(1)(a) of the GDPR. On the other hand, if the consent of the data subject does not meet the GDPR conditions for consent (e.g., it is implied and not

[34] §48 of the Recommendations.

[35] §116 of the Recommendations.

[36] §117 of the Recommendations.

express, not freely-given, not specific or not informed), it is uncertain that this contractual measure would amount to a substantially equivalent level of protection as that afforded by EU law.

The EDPB should consider removing such data subject consent requirement or further elaborating on the purpose of obtaining such consent.

10. Coordinated Approach with the European Commission on the New SCCs

The EDPB should consider taking advantage of the publication of the New SCCs to coordinate its approach more closely with the European Commission. As explained above, the EDPB should in particular consider adopting a risk-based approach to assessing the law and practice of third countries taking into account the same factors as those laid out in the New SCCs (see point 2 above), and aligning its positions on onward transfers (see point 5 above) and pseudonymisation (see point 7 above) with the one reflected in the New SCCs.

The EDPB should also identify the supplementary contractual measures described in the Recommendations that are incorporated in the New SCCs, in which case they should be viewed as part of the chosen transfer tool (and therefore not as "supplementary" measures) if SCCs are used by the parties. Other contractual measures suggested by the EDPB would then be viewed as optional provisions which the parties may choose to include in the SCCs or other transfer tools to further increase their chances that the "essentially equivalent" standard will be met

* * *

AFME and SIFMA greatly appreciate the opportunity to provide comments on the Recommendations and the EDPB's consideration of these issues and would be pleased to discuss them in greater detail. If you have any questions or need any additional information, please contact Aleksandra Wojcik, Aleksandra.Wojcik@afme.eu, and Melissa MacGregor, mmacgregor@sifma.org.