AFME and SIFMA joint comments to the European Commission's draft implementing decision on standard contractual clauses for the transfer of personal data to third countries pursuant to regulation (EU) 2016/679

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 European Commission's draft implementing decision (the "Implementing Decision") on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 (the "New SCCs") published by the European Commission on November 12, 2020[3] as input for the final Implementing Decision and New SCCs[4].

Pursuant to the General Data Protection Regulation (EU) 2016/679 (the "GDPR") and 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 European Commission's New SCCs were expected to provide:

- a robust framework for the transfer of personal data to third countries, taking into account the GDPR as well as the increased complexity and frequency of data transfers in 2020;

[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://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12741-Data-protection-standard-contractual-clauses-for-transferring-personal-data-to-non-EU-countries-implementing-act-

[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

- a mechanism to ensure the continuity of essential data flows, in particular in light of the uncertainty generated by the *Schrems II* judgment; and
- consistency with the guidance issued by the European Data Protection Board (the "EDPB"), including the EDPB's Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data on November 11, 2020 (the "Recommendations").[5]

We appreciate the European Commission's use of a modular approach to create a comprehensive framework under which data importers and data exporters can contract, irrespective of their qualification as controller or processor. However, AFME's and SIFMA's members have concerns about the practical implementation and interpretation of the New SCCs, in their current form, which may give rise to legal uncertainty and disruptions to data flows in the future. In addition, AFME's and SIFMA's members would like to take this opportunity to request that the European Commission encourage the EDPB to align their Recommendations with the New SCCs.

Our comments below intend to provide constructive suggestions in an attempt to ensure clarity and certainty, while promoting the interests of data exporters, importers and data subjects and complying with the standards set out in *Schrems II* and the GDPR.

Executive Summary

AFME and SIFMA urge the European Commission to consider the following when preparing the final version of the Implementing Decision and the New SCCs:

1. ***Enable Existing SCCs to remain in force until their expiration or termination by the parties or grant a three-year grace period*.** While the Implementing Decision provides for the immediate repeal of Decision 2001/497/EC and Decision 2010/87/EU (the "Existing SCCs") and a one-year grace period in which to continue to rely on them,[6] the CJEU in *Schrems II* upheld the Existing SCCs and gave the parties the ability to adopt "*additional safeguards*" to cure the issues created as a result of the surveillance laws of the data importer's country.[7] The repapering of the Existing

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

[6] Articles 6(1), 6(2) and 6(3) of the Implementing Decision.

[7] "It is therefore, above all, for that controller or processor to verify, on a case-by-case basis and, where appropriate, in collaboration with the recipient of the data, whether the law of the third country of destination ensures adequate protection, under EU law, of personal data transferred pursuant to standard data protection clauses, by providing, where necessary, additional safeguards to those offered by those clauses."(*Schrems II*, §134).

SCCs following the one year grace period is potentially, therefore, unnecessary and unduly costly. The Implementing Decision should therefore allow for the use of Existing SCCs on a continuing basis (subject to compliance with the principles of *Schrems II*) or grant a three-year grace period.

2. ***Clarify that the data controller is not a party to the New SCCs in the case of processor-to-processor transfer*.** The New SCCs should be clarified to explain that inclusion of the details of the data controller (in the context of a processor to processor transfer) in Annex I.A, does not cause such controller to be considered a party to the New SCCs (as currently suggested by the wording of Section I Clause 1(b) of the New SCCs).

3. ***Enable the parties to amend the New SCCs to change the purpose of the transfer*.** Modules One, Two and Three of the New SCCs each limit the data importer's processing of personal data it receives under the New SCCs to the purposes described in the description of the transfer (Annex I.B) (or, with respect to Module One, with the consent of the data subject). The ability to amend the description of the transfer to take into account the evolving relationship between data importers and data exporters over time should, however, be acknowledged, provided that such change is consistent with the GDPR.

4. ***Align the data breach notification standard and requirements with those of the GDPR*.** Module One, which applies to controller-to-controller transfers, provides that the data importer must notify the (i) data exporter, (ii) competent supervisory authority, and (iii) data subjects concerned, in the event that a data breach is "*likely to result in significant adverse effects*". The notification standard needs to be clarified, given it is a departure from the thresholds for breach notification to the competent supervisory authority and data subjects provided for in articles 33 and 34 of the GDPR. Additionally, the obligation to notify the data exporter is unnecessary, not provided for by the GDPR and should not be required under the New SCCs.

5. ***Set appropriate pseudonymisation standards*.** Modules Two and Three, which apply to controller-to-processor and processor-to-processor transfers, respectively, provide that where pseudonymisation is applied to the transferred personal data, the "additional information for attributing the personal data to a specific data subject" shall, where possible, remain under the exclusive control of the data exporter. An exclusive control arrangement may not, however be

feasible and instead this requirements should focus on ensuring the data *importer* is unable to access the information necessary to identify the relevant data subjects.

6. ***Clarify the flow-down of provisions in the case of onward transfers*.** The New SCCs provide that a data importer may not make an onward transfer of the data unless the third party recipient of the data agrees to be bound by "*these Clauses*". The New SCCs should be clarified so that it is clear that the reference to "*these Clauses*" is intended to allow for the selection of the Module applicable in the context of the onward transfer.

7. ***Grant the parties additional flexibility with respect to audits*.** Modules Two and Three, which apply to controller-to-processor and processor-to-processor transfers, respectively, incorporate detailed rights and obligations in connection with compliance audits. In particular, the provisions provide for certain allocations of costs and prescribe certain logistical elements of the audit. Such rights and obligations should be left open to negotiation between the parties, in order that the New SCCs do not cut across any existing commercial arrangements or regulatory or contractual confidentiality obligations.

8. ***Enable the parties to rely on the data exporter instead of the data controller in certain Module Three provisions (processor-to-processor transfers).*** Throughout Module Three, references are made to the controller in a way that supposes there would be a direct line of communication between the data importer (the sub-processor) and the original controller. Given the possibility that no such line of communication has been or can be established, the New SCCs should clarify that (i) the data importer can rely solely on the instructions of the data exporter (being the instructions of the controller, passed down via the data exporter), and (ii) the data importer will have discharged its duties (i.e., in connection with data breaches or data subject access requested) where it has made a notification to the data exporter.

9. ***Clarify the scope of application of the clauses applicable to processor-to-controller transfers (Module Four).*** The precise application of the New SCCs to processor-to-controller transfers is unclear. While certain Module Four provisions incorporate explanatory notes as to their application, others do not. It is not clear whether the European Commission intended for the processor-to-controller clauses to apply only where personal data originating in the EU is combined with non-EU data, or a to a broader set of circumstances (including where the processor is transferring personal data solely originating in the EU). The New SCCs (and

explanatory notes) should be clarified to ensure consistent and comprehensive application of the New SCCs to processor to controller transfers.

10. ***Qualify the requirement to notify the competent supervisory authority if obligations cannot be fulfilled*.** The New SCCs require the data exporter to notify the competent supervisory authority in the event that the data importer has indicated that it cannot comply with its obligations. This notification requirement should be qualified so that it applies only where the parties cannot find a way of curing the issued through the application of additional measures and safeguards. This is in-line with the principle of accountability under the GDPR and will reduce unnecessary uncertainty associated with making the notification to the competent supervisory authority.

11. ***Add a threshold consistent with the GDPR for notifying data subjects and data exporters in case of access to the transferred data by a public authority in the recipient country*.** The New SCCs require the data importer to notify the data exporter and, where possible (with the help of the data exporter), data subjects, in the event that a public authority requests access to personal data or directly accesses personal data, in accordance with the laws of the country of destination. There is no limitation or threshold with respect to this notification obligation (even where the request does not present any risk to the rights and freedoms of data subjects). The New SSCs should be revised to incorporate an appropriate threshold for such obligation (modelled on the notification threshold of supervisory authorities and data subjects in the event of a personal data breach pursuant to articles 33 and 34 of the GDPR).

12. ***Take into account the likelihood of access to the transferred data by public authorities in the recipient countries*.** The New SCCs require that the parties to the transfer must warrant that they have no reason to believe that the laws applicable in the third country will prevent the data importer from fulfilling its obligations under the clauses. The New SCCs provide a list of the various considerations that are required to be taken into account as part of this analysis. However, this list should not be exhaustive and (in line with the risk-based approach promoted by the GDPR) should allow for an assessment of the likelihood of access to the transferred data by the public authorities in the recipient country.

13. ***Qualify the requirement to "exhaust all remedies" to challenge a request to access data by a public authority.*** The New SCCs require data importers to review the legality of a public authority request to access personal data and "*exhaust all remedies*" available to it to challenge the request. No account is taken of the likelihood that such requests will give rise to risks to the rights and freedoms of data subjects and the requirement to exhaust all remedies is extremely

onerous and potentially costly. The New SCCs should include a threshold for the obligation to challenge a public authority request (based on the likelihood of any harm to data subjects) and the obligation should be limited to taking reasonable steps rather exhausting all remedies.

14. ***Grant the parties additional flexibility to allocate liabilities between them*.** The New SCCs provide that each party shall be liable to the other parties for any material or non-material damages it causes by its breach of the New SCCs. This, however, should be treated as a purely commercial matter between two private parties and should not be determined by the European Commission. In addition, the requirement for the data importer to agree to a third party beneficiary clause with the sub-processor may be unenforceable or be in conflict with the local laws. This requirement should, therefore, be qualified so that it applies only where it is where consistent with applicable local law.

15. ***Provide for a single competent supervisory authority when the data exporter is subject to the GDPR pursuant to article 3(2).*** Where a data exporter is required to comply with the GDPR by virtue of its article 3(2) (i.e., when processing of the transferred data relates to the offering of goods or services or the monitoring of behaviour of data subjects in the EU), the supervisory authority with responsibility for ensuring the data exporter's compliance with the GDPR as regards the transfer is the supervisory authority of the member state where the data subjects whose personal data are transferred are located. This could result in the data exporter owing obligations to multiple supervisory authorities. The New SCCs should instead provide for a mechanism by which the a single supervisory authority can be selected (based on the location of the majority of the data subjects).

16. ***Coordinate with the EDPB to align the Recommendations with the New SCCs*.** We encourage the European Commission to ensure that the Recommendations published by the EDPB are aligned with the approach the European Commission intends to take in connection with the New SCCs.

* * *

1. Enable Existing SCCs to Remain In Force Until their Expiration or Termination or Grant a Three-Year Grace Period

The Implementing Decision provides for the immediate repeal of the Existing SCCs and a one-year grace period in which to continue to rely on them.[8] The Implementing Decision provides that this grace period shall apply only to contracts entered into prior to the date of the Implementing Decision and only so long as the contract has not been modified (except for modifications to provide for necessary supplementary measures to ensure compliance with the appropriate safeguards requirement under article 46 of the GDPR).

However, the CJEU in *Schrems II* upheld the Existing SCCs and gave the parties the ability to adopt "*additional safeguards*" when such step is warranted by the surveillance laws of the data importer's country.[9] Arrangements taken pursuant to the Existing SCCs may, therefore, already be in compliance with the GDPR as well as the principles of *Schrems II* or could be modified to bring them in line with such principles. The repapering of the Existing SCCs following the one year grace period is potentially, therefore, unnecessary and unduly costly.

We would therefore urge the European Commission to consider:

- clarifying that use of the Existing SCCs may continue for the duration of the existing contractual arrangement between the parties, subject to the imposition of any supplementary measures necessary to ensure compliance with Article 46 and the principles of Schrems II; or
- alternatively, providing for a longer grace period of three years, in light of the fact that: (i) data exporters may, instead of entering into New SCCs, decide to amend the Existing SCCs in order to adopt supplementary contractual measures in accordance with *Schrems II*, as indicated by the EDPB in its Recommendations, and (ii) organisations have already recently gone to great lengths to update their contractual arrangements to comply with article 28 of the GDPR as well as the Schrems II judgment and any unnecessary repapering exercise should be avoided where arrangements are in technical compliance with the GDPR.

[8] Article 6(1), Article 6(2) and Article 6(3) of the Implementing Decision.

[9] "It is therefore, above all, for that controller or processor to verify, on a case-by-case basis and, where appropriate, in collaboration with the recipient of the data, whether the law of the third country of destination ensures adequate protection, under EU law, of personal data transferred pursuant to standard data protection clauses, by providing, where necessary, additional safeguards to those offered by those clauses."(*Schrems II*, §134).

2. Clarify that the Data Controller Is Not a Party to the New SCCs in the Case of Processor-to-Processor Transfer

Section I, Clause 1(b) of the New SCCs explains that the parties to the New SCCs are the entities listed in Annex I.A. As well as setting out the data exporter and data importer parties, Annex I.A also requires the inclusion of the details of the relevant controller(s) in connection with processor to processor transfers. This gives rise to the impression that, in connection with a processor to processor transfer, the underlying controller is also a party to the New SCCs.

On the understanding that the underlying controllers are not intended to be parties to the New SCCs in this context, we request that the European Commission clarify Section I Clause 1(b) of the New SCCs so that the definition of "Parties" does not reflect the underlying data controller(s) listed in Annex I.A.

3. Enable the Parties to Amend the New SCCs to Change the Purpose of the Transfer

Each of Modules One, Two and Three of the New SCCs contains a provision regarding the purpose of processing permitted under the New SCCs or incorporate the principle of purpose limitation,[10] which provides that the data importer may process personal data it receives under the New SCCs only for the purposes described in the description of the transfer (Annex I.B) or, with respect to Module One, with the consent of the data subject. The ability to amend the description of the transfer to take into account the evolving relationship between data importers and exporters over time, is not acknowledged.

To reduce the administrative burden on the parties to the New SCCs as much as possible, without reducing the efficacy of the New SCCs or the level of protection they provide for data subjects, the European Commission should consider adding language to the New SCCs to confirm that the description of the transfer can be updated, from time to time, upon the agreement of the parties (signified by the dating and signing of a new description of the transfer).

4. Align the Data Breach Notification Standard and Requirements with Those of the GDPR

The GDPR provides for the following data breach notification thresholds: controllers must (i) notify supervisory authorities of a data breach unless such data breach is unlikely to result in a risk to the rights and freedoms data subjects[11], and (ii) notify data subjects of a data breach where it is likely to result in a high risk to their rights and freedoms[12]. Section II, Module One (controller to controller), Clauses 1.5(d)

[10] Section II, Module One, Clause 1.1; Section II, Module Two, Clause 1.2; and Section II, Module Three, Clause 1.2 (New SCCs).
[11] Article 33(1) of the GDPR.
[12] Article 34(1) of the GDPR.

and (e), however, provide that the data importer must notify the (i) data exporter, (ii) competent supervisory authority, and (iii) data subjects concerned, where the data breach is "*likely to result in significant adverse effects*".

It is not clear whether the European Commission intends for the breach notification threshold set out in the New SCCs to be a lower or higher threshold than the breach notification thresholds provided for by the GDPR, nor whether the assessment of "*significant adverse effects*" is intended to apply only to data subject rights and freedoms, or to a broader range of interests. The incorporation of a new threshold is likely to lead to confusion and uncertainty.

Additionally, as noted above, the notification obligation upon a data importer (controller), includes the obligation to inform the data exporter (controller). The obligation for one controller to notify another is a new obligation that is not otherwise found in the GDPR. If the data importer is an independent controller, its breach notification obligations under the GDPR are its own responsibility. If the data exporter and data importer are joint controllers of the relevant processing, the "arrangement" to be agreed between them pursuant to article 26 of the GDPR should set out their respective responsibilities regarding notification obligations.[13]

We would therefore encourage the European Commission to:

- clarify its intention with respect to the meaning of "*likely to result in significant adverse effects*", or consider aligning the breach notification threshold in the New SCCs with the thresholds provided under the GDPR; and
- remove the obligation on the data importer controller to notify the data exporter controller, under Section II, Module One, Clause 1.5(d), which is not a requirement of the GDPR and would otherwise be dealt with in a joint control arrangement, where applicable.

5. Set Appropriate Pseudonymisation Standards

Section II, Modules Two and Three (controller to processor and processor to processor transfers, respectively), Clause 1.6 provides that the data exporter and data importer should consider pseudonymisation as a means to ensure an appropriate level of security for personal data (where pseudonymisation would not prevent the data importer from fulfilling the purpose of the processing). Clause 1.6 also requires that where pseudonymisation is used, the "*additional information for attributing*

[13] Article 26(1) of the GDPR provides that joint controller "shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14, by means of an arrangement between them […]".

the personal data to a specific data subject" ("Additional Information") shall, where possible, remain under the exclusive control of the data exporter.

However, agreeing to exclusive control by the data exporter may not be feasible. The Additional Information may not be in the hands of the data exporter who could have received the data in pseudonymised form to begin with. Alternatively, as provided for in the Recommendations, the data could be subject to split or multi-party processing[14] (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 European Commission should recognize 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).

We therefore encourage the European Commission to revise the requirement in Clause 1.6 (of Section II, Modules Two and Three) so that the onus is on the data *importer* to be precluded from accessing Additional Information, rather than requiring that the data exporter have exclusive control over Additional Information (which may not be realistic or feasible in the circumstances).

6. Clarify the Flow-Down of Provisions in the Case of Onward Transfers

Section II, Module One (controller to controller), Clause 1.7 provides that the importer may not make an onward transfer unless the third party recipient of the data agrees to be bound by "*these Clauses*". Clause 1.7 does not provide a mechanism by which the clauses can be selected/revised on the modular basis to ensure the appropriate flow-down of provisions depending on the role (controller vs. processor) being undertaken by the onward data importer.

For example, where (in the controller to controller context) the importer is making the onward transfer to a processor, the Module One (controller to controller) clauses may not be appropriate and should instead be substituted by the Module Two controller to processor clauses for the purpose of the onward transfer.

Equally, in Section II, Module Two (controller to processor) and Section II, Module Three (processor to processor), similar provisions apply (requiring that recipients of onward transfers of personal data must be made subject to "*these Clauses*"). In the event that the original controller instructs the processor to make an onward transfer to a third party *controller*, "these Clauses" may be more appropriately substituted for the provisions of Module Four.

[14] Paragraph 86 of the Recommendations.

The European Commission should therefore consider clarifying that where onward transfers are permitted, the exporting party must ensure the *appropriate* contractual clauses are imposed, depending on the nature of the data importer.

7. Grant the Parties Additional Flexibility With Respect to Audits

Section II, Modules Two and Three (controller to processor and processor to processor transfers, respectively), Clauses 1.9(d) and (e), set out the rights and obligations with respect to compliance audits. More specifically, these Clauses provide that:

- the data importer must allow for and contribute to reviews of data files and documentation, or audits of the processing activities covered by the contract (in particular, if there are indications of non-compliance);
- in determining whether to review or audit, the data exporter may take into account any certifications held by the data importer;
- the data exporter may mandate an independent third party to execute the audit at its own cost, or the data importer can mandate the audit by an independent third party at its own cost; and
- audits can include on-premises inspections, to be carried out with reasonable notice.

While the New SCCs are prescriptive, various aspects of the audit and inspection arrangements between a controller and a processor, or a processor and its sub-processor, are context specific and should be subject to commercial negotiation between the parties. For example, it may not be appropriate in a particular context to permit on premises inspections and the parties may have particular limitations due to confidentiality obligations owed to third parties. Additionally, the cost allocation of inspections and audits should be a matter for negotiation and may be reflected in the price of services provided / received. What constitutes reasonable notice, as well the details of the conduct of audits and inspections (i.e., the appropriate qualification of personnel, timing of visits, limitations on business disruption) should also be a matter for the parties to negotiate.

In order to allow for flexibility in the context of commercial negotiations, we encourage the European Commission to provide additional optionality with respect to audits, including:

- allowing the parties to determine the allocation of costs;
- allowing the parties to select from a range of audit options (including, but not limited to on-premises inspections) to best fit the context; and

- allowing space for the parties to add additional restrictions or notice requirements in order to manage business disruption and ensure the availability of comprehensive information so that audits can be conducted successfully and efficiently.

8. Enable the Parties to Rely on the Data Exporter Instead of the Data Controller in Certain Module Three Provisions (Processor-to-Processor Transfers)

Throughout Section II, Module Three, references are made to the controller in a way that supposes there would be a direct line of communication between the data importer (the sub-processor) and the original controller.

For example (all Clauses referred to below are found in Section II, Module Three of the New SCCs):

- Clause 1.1 provides that the data importer shall process data only on documented instructions from the controller (as well as any additional documented instructions from the data exporter);
- Clause 1.6 provides that in the event that the data importer suffers a data breach, it must notify the data exporter and "*where appropriate, the controller*";
- Clause 1.8 provides that the data importer shall only disclose the personal data to a third party on the basis of documented instructions from the controller;
- Clause 4(a) provides that where a data importer wishes to appoint a sub-processor or make changes to a pre-approved list of sub-processors, the data importer will inform the data controller;
- Clause 5(a) and (b) provide that the data importer will notify the controller (where appropriate) of any request or inquiry received directly from a data subject and shall provide the data controller with assistance to allow the controller to respond to the data subject.

While it is possible that the controller will provide its instructions to the data importer directly, in many cases the data importer will not be in direct contact with the controller and it is more likely that the instructions for processing will be passed on to the data importer via the data exporter. There could be practical reasons for such delegation arrangements (i.e., delegation to the data importer by data exporter rather than by the controller directly); for example, there could be language barriers and time zone issues that preclude direct communications between the data importer and the controller. It is also possible that the data importer is not aware of the identity of the data controller and cannot, therefore (i) seek its permission to appoint a sub-processor, or (ii) notify it in the event of a breach of a data subject request, for example.

We therefore encourage the European Commission to clarify that:

- while direct instructions from the data controller may be feasible, the data importer can rely solely on the instructions of the data exporter (being the instructions of the controller, passed down via the data exporter); and
- the data importer will have discharged its data breach and data subject access notification duties where it has notified such event to the data exporter and does not also have to provide notification to the controller.

9. Clarify the Scope of Application of the Clauses Applicable to Processor-to-Controller Transfers (Module Four)

The explanatory note to Section II, Clauses 2 and 3 provides that these provisions of the New SCCs apply in connection with processor-to-controller transfers (Module Four) only where the EU processor combines the personal data received from the third country with personal data collected by the processor in the EU.

Elsewhere in the New SCCs (for example Section III, Clause 1(d)), the Module Four provisions are not accompanied by an explanatory note (and, therefore, it is not specified that the Module Four provisions apply only where EU data is combined with data originating in a third country).

With respect to the Module Four provisions, therefore, there are number uncertainties:

- should Section II, Clauses 2 and 3 not also apply where the entirety of the personal data collected by the EU processor originated in the EU (i.e., where the personal data is entirely EU personal data collected upon the instruction of the non-EU controller);
- where the processor did combine data originating in the EU with data received from a third country, should Section II, Clauses 2 and 3 not clarify that the application of these provisions is limited to the new combined data set (and not also to the data received from the third country in its non-combined form); and
- with respect to the Module Four provisions which are not accompanied by an explanatory note, is it the European Commission's intention that such provisions apply on a blanket basis (or should they also be qualified by the same explanatory note found in Section II, Clauses 2 and 3)?

We encourage the European Commission to:

- clarify its existing notations so that (i) personal data originating entirely in the EU is clearly within scope, and (ii) where personal data originating in the EU is combined with personal data received from a third country, the provisions apply only to the new combined data set; and
- include a notation for any other Module Four provisions so that it is clear that their scope of application is limited to data originating in the EU or new data sets comprising both EU and non-EU data.

10. Qualify the Requirement to Notify the Competent Supervisory Authority if Obligations Cannot be Fulfilled

Section II, Clause 2(f) requires the data exporter to notify the competent supervisory authority in the event that the data importer cannot comply with its obligations under the New SCCs. This notification requirement exists even where the parties have determined that it is possible to continue with the transfer based on the application of additional measures and safeguards. The data exporter must suspend the data transfer if the competent supervisory authority instructs it to do so.

Consultation with the competent supervisory authority is not generally required under the GDPR in connection with data transfers outside the EU or with respect to the use of SCCs (in line with the overarching principle of accountability pursuant to article 5(2) of the GDPR). It is not clear why, therefore, the data exporter is required to notify the competent supervisory authority in a case where it has applied additional measures to safeguard the transfer (in line with the requirements of article 46 of the GDPR) and considers any concerns with respect to the transfer, remedied.

The notification process is potentially burdensome and could lead to uncertainty following notification, pending the competent supervisory authority's findings. This may lead to disruptions to data flows, even where additional measures have been appropriately applied to safeguard the personal data.

We therefore encourage the European Commission to remove this requirement in cases where the data exporter has determined that appropriate safeguards have been or can be put in place to remedy the concerns raised by the data importer, such that the requirements of article 46 of the GDPR can be satisfied.

11. Add a Threshold Consistent with the GDPR for Notifying Data Subjects and Data Exporters in Case of Access to the Transferred Data by a Public Authority in the Recipient Country

Section II, Clause 3.1(a) requires the data importer to notify the data exporter and, where possible (with the help of the data exporter), data subjects, in the event that a public authority requests access to

personal data or directly accesses personal data, in accordance with the laws of the country of destination. There is no limitation or threshold with respect to this notification obligation.

A notification is required, therefore, even where the personal data accessed is pseudonymised such that access to the data would not present a risk to the rights and freedoms of the data subject, or where the potential (or even likely request) for the personal data form the public authority was pre-notified to the data subject by the data exporter (for example, where the transfer was made in the expectation of publication authority access, such as in connection with a regulatory or tax filing).

Taking into account the above, in order to reduce the burden for data importers where the public authority access in question does not give rise to concerns for the rights and freedoms of data subjects, we encourage the European Commission to introduce the following thresholds:

- *notification to the data exporter* – the European Commission should provide for a threshold similar to that set out in article 33 of the GDPR; and
- *notification to data subjects* - the European Commission should provide for a threshold similar to that set out in article 34 of the GDPR.

12. Take Into Account the Likelihood of Access to the Transferred Data by Public Authorities in the Recipient Countries

Under Section II Clause 2, parties to the transfer must warrant that they have no reason to believe that the laws applicable in the third country will prevent the data importer from fulfilling its obligations under the clauses. Clause 2(b) lists various considerations that are required to be taken into account as part of this analysis.

While this clearly promotes a nuanced, case-by-case, risk based assessment, the list of relevant considerations at Clause 2(b) appears to be exhaustive and does not provide for any assessment of the likelihood of a theoretical risks arising. By contrast, the GDPR takes into account the "likelihood" of a risk crystalizing before imposing obligations, in a number of cases. For example:

- 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;[15]

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

- 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;[16] 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[17] and is required to be made to the data subjects only if it is likely to result in a high risk to them.[18]

The ability to carry out a risk based approach, including the likelihood of a threat materialising, is central to ensuring the continued flow of personal data where risk is theoretical or proportionate. Accordingly, we encourage the European Commission to clarify that:

- the list in Clause 2(b) is non-exhaustive; and
- alternatively or additionally, that an assessment of the likelihood of access be incorporated into the list of relevant considerations of a third country's laws and practices.

13. Qualify the Requirement to "Exhaust All Remedies" to Challenge a Request to Access Data by a Public Authority

Section II, Clause 3.2(a) requires the data importer to review the legality of a public authority request to access personal data and "*exhaust all remedies*" available to it to challenge the request.

This requirement applies irrespective of the nature of the request or the personal data requested. No account is taken of the likelihood of any risks to the rights and freedoms of data subjects. As described under section 12 above, this departs from risk-based approach central to the GDPR.

In the absence of a proportionate approach, the requirement to exhaust all remedies is extremely onerous and potentially costly. It may result in data importers being reluctant to process EU personal data, which will in turn give rise to disruptions to international data flows.

We therefore encourage the European Commission to:

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

[17] Article 33 and recital (85) of the GDPR.

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

- introduce a threshold for the obligation to challenge a public authority request, taking into account the likelihood of harm to data subjects; and
- qualify the obligation by a requirement to "take reasonable steps" rather than to "*exhaust all remedies*".

14. Grant the Parties Additional Flexibility to Allocate Liabilities Between Them

Section II, Clause 7 provides that each party shall be liable to the other parties for any material or non-material damages it causes by its breach of the New SCCs.

This should be treated as a purely commercial matter between two private parties and should not be determined by the European Commission. It may not align, for example, with the commercial arrangements in connection with the exchange of services agreed by the parties. As this matter does not impact the compensation that would be available to data subjects, it should be a matter left to the parties to determine.

We therefore encourage the European Commission to allow the liability provisions vis-à-vis the parties to be determined by the parties.

Additionally, Section II, Clause 4(e), Modules Two and Three (controller to processor and processor to processor transfers, respectively), requires the data importer to agree a third party beneficiary clause with any sub-processor it appoints (in favour of the data exporter, in the event of the data importer's bankruptcy). However, this requirement does not acknowledge the possibility that such a clause may be unenforceable or in conflict with the local laws. This requirement should, therefore, be qualified so that it applies only where consistent with applicable local law.

We therefore encourage the European Commission to add this qualification to Section II, Clause 4(e).

15. Provide for a Single Competent Supervisory Authority When the Data Exporter is Subject to the GDPR Pursuant to Article 3(2)

Under Section II, Clause 9(a), where the data exporter is located outside of the European Economic Area but is required to comply with the GDPR by virtue of article 3(2) of the GDPR (i.e., when processing of the transferred data relates to the offering of goods or services or the monitoring of behaviour of data subjects in the EU), the supervisory authority with responsibility for ensuring the data exporter's

compliance with the GDPR as regards the transfer is the supervisory authority of the member state where the data subjects whose personal data are transferred are located.

No mechanism is provided for a single supervisory authority to be chosen in the event that the transfer relates to data subjects in multiple member states. Therefore, even the presence of a single data subject in a member state would require the data exporter to be subject to the jurisdiction of that member state's supervisory authority and be required to provide notifications to such supervisory authorities (for example, in the event of a data breach). This could result in obligations being owed to multiple supervisory authorities.

We encourage the European Commission to incorporate a mechanism whereby a single competent supervisory authority can be selected based on the location of the majority of the data subjects in question.

16. Coordinate with the EDPB to Align the Recommendations With the New SCCs

We encourage the European Commission to ensure that the Recommendations published by the EDPB are aligned with the approach the European Commission intends to take in connection with the New SCCs. In particular, the European Commission should coordinate with the EDPB to ensure that the Recommendations are consistent with the New SCCs, including on the following aspects:

- liability for onward transfers (which under the Recommendations rests with the original data exporter);
- the inclusion of a risk-based approach to assessing the law and practice of third countries (which is not permitted under the Recommendations, in contrast to the approach promoted in Section II, Clause 2(b) of the New SCCs);
- the pseudonymisation standards (which, under the Recommendations, require that the additional information required to re-identify the data subjects be held "exclusively by the data exporter" while the New SCCs recognise that this may not always be possible); and
- the concept of supplementary measures (which the Recommendations explain should be introduced in addition to the chosen transfer tool, but which have already been incorporated in many cases into the New SCCs).

* * *

AFME and SIFMA greatly appreciate the opportunity to provide comments on the Implementing Decision and the New SCCs and the European Commission'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.