December 10, 2020

BSA comments on the Commission implementing decision on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679

BSA | The Software Alliance ("BSA"),[1] the leading advocate for the global software industry, welcomes the opportunity to provide feedback on the European Commission's draft new standard contractual clauses ("SCCs") for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679.

BSA members are enterprise software companies that create the technology products and services that other businesses use. For example, BSA members provide business-to-business tools including cloud storage services, customer relationship management software, human resource management programs, identity management services, and workplace collaboration software. Businesses entrust some of their most sensitive information—including personal data—with BSA members. Our companies work hard to keep that trust. As a result, privacy and security protections are fundamental parts of BSA members' operations.

As enterprise software companies, BSA members help companies worldwide use digital tools to provide products and services to their customers. Those customers – and the companies that serve them – rely on the ability to send data across international borders, subject to appropriate privacy projections. Cross-border transfers are needed for a range of consumer-facing services such as e-commerce (which depend on moving data across borders to track and fulfil orders), and business-to-business services across industries ranging from automotive to agriculture, finance, healthcare, manufacturing, human resources, and many others. Indeed, companies that operate globally must send data across international borders to perform daily business transactions like processing payroll, sending emails, or storing documents on cloud-hosted servers. This work has taken on increased importance amid the COVID-19 pandemic, which has spurred companies in all industries to increasingly rely on remote workplace tools and cloud-based technologies and has enabled medical researchers and hospitals worldwide to coordinate their research and treatment efforts.

BSA members have long recognized the importance of responsible international data transfers. In 2016, BSA was granted permission to participate as an amicus in *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems* ("*Schrems II*"), and we participated before both the Irish High Court and the Court of Justice of the European Union ("CJEU").[2] In those proceedings,

[1] BSA | The Software Alliance (www.bsa.org) is the leading advocate for the global software industry before governments and in the international marketplace. Its members are among the world's most innovative companies, creating software solutions that spark the economy and improve modern life. With headquarters in Washington, DC, and operations in more than 30 countries, BSA pioneers compliance programs that promote legal software use and advocates for public policies that foster technology innovation and drive growth in the digital economy.
BSA's members include: Adobe, Akamai, Atlassian, Autodesk, Bentley Systems, Box, Cadence, Cloudflare, CNC/Mastercam, DocuSign, Dropbox, IBM, Informatica, Intel, Intuit, MathWorks, McAfee, Microsoft, Okta, Oracle, PTC, Salesforce, ServiceNow, Siemens Industry Software Inc., Sitecore, Slack, Splunk, Trend Micro, Trimble Solutions Corporation, Twilio, and Workday.

[2] *See* https://www.bsa.org/news-events/news/bsa-welcomes-irish-high-courts-decision-to-grant-bsa-amicus-status.

Avenue des Arts 44
1040 Brussels
Belgium

P +32 (0)2 274 13 10
W bsa.org
EU Register of Interest Representatives 75039383277-48

we emphasized the importance of the Standard Contractual Clauses ("SCCs"), which provide a vital privacy-protective mechanism that is used by millions of companies—based in countries worldwide—that transfer data in and out of Europe. Nearly 90 percent of companies transferring data out of the EU rely on SCCs.[3]

We welcome these new draft SCCs aiming at updating the existing SCCs in light of the GDPR, ensuring that they are reflecting the realities of the digital environment and account for the variety of transfers, and addressing the CJEU's requirement emanating from the 16 July 2020 Schrems II decision, in particular with regard to the necessity for exporters and importers of data to assess possible access to data by public authorities in the third country and identifying appropriate supplementary measures where needed.

We respectfully submit the comments below in response to the Commission's consultation on the New SCCs.

1. **Making the New SCCs more flexible is a positive development. We encourage the Commission to make further changes to ensure the New SCCs can be used in the widest range of scenarios.**

We welcome the Commission's efforts to ensure that the New SCCs provide adequate safeguards for all types of transfers—whether controller-controller, controller-processor, processor-controller or processor-processor.[4] We further welcome the indications in the draft that the New SCCs can be used where a company located outside the EEA is directly subject to the GDPR and will transfer data to another company located outside the EEA. Data transfers take many shapes and forms, and these improvements will allow the New SCCs to be used in a variety of transfer scenarios.

However, the draft SCCs leave some areas of ambiguity about their application and use. In particular, it is not clear which modules to use where a controller that is located in the EEA appoints a processor outside the EEA to collect data directly from EEA data subjects. It is also unclear whether a data exporter and data importer must sign multiple instances of the draft SCCs if they have multiple roles.

> For example, a hosting provider located in India may act as a processor to host EEA clients' data, and as a controller for certain value-added services it provides. Would this provider be able to enter into a single set of the new SCCs with each customer (with multiple versions of Annex I.B) or should it enter into a different set for each type of transfer?

We encourage the Commission to clarify these points. The New SCCs should ultimately be flexible enough to allow companies to use them in each of these situations.

In addition, certain aspects of specific clauses in the New SCCs also limit their flexibility and should be revised:

- *Termination rights over the whole "contract."* The New SCCs grant the data exporter the right to terminate the "contract" — i.e. the underlying commercial terms — in certain circumstances (*see e.g.*, Section II, clauses 2(b)(i) and 2(f), Section III, clause 1(c)). Large commercial contracts often cover multiple services, many of which may not involve

[3] IAPP-EY Annual Governance Report 2019 (Nov. 6, 2019), available at: https://iapp.org/resources/article/iapp-ey-annual-governance-report-2019/ (stating approximately 88% of companies transferring data out of the EU rely on SCCs).

[4] The new SCCs also make it possible for more than two parties to sign standardized contracts, which can be helpful in providing additional flexibility.

processing personal data. Data exporters should not have an unfettered right to terminate the contract for all services. Instead, as envisaged by the Current SCCs, they should generally be limited to terminating the relevant transfers (*e.g.*, those in relation to which the importer can no longer comply with the SCCs);

- *Relationship with existing controller-processor terms*. Many companies have already entered into bespoke controller-processor agreements that reflect the requirements of Article 28(3) GDPR and are appropriate to their own relationship. Companies should be able to rely on these provisions over and above the terms set out in Section II, C-P and P-P modules, clauses 1, 4 and 5, provided that they do not directly conflict with these clauses.
- *Explicit consent for onward transfers*. Section II, C-C module, clause 1.7 requires the data importer to obtain the explicit consent from the data subject in certain scenarios. In many situations, and in particular in a B2B context, the importer may not have a direct relationship with the data subject so it remains unclear how the data importer can obtain consent for data that are transferred on behalf of and by the data exporter. We recommend changing this obligation so that the data exporter obtains explicit consent from the data subject and informs the data importer.
- *Good faith cooperation*: The language in Section II, C-P module, clause 1.6(d) that requires the data importer to cooperate in good faith with and assist the data exporter "in any way necessary" is vague and could lead to extensive and unattainable interpretations. We would recommend clarifying and qualifying this language to limit potentially undue burdens – maybe to "in a way that can be reasonably expected."
- *Inconsistency with joint controllership provisions*. Section II, C-C module, clause 5 rigidly requires controller-importers to respond to requests they receive from data subjects wishing to exercise their rights. This is inconsistent with how the GDPR envisages joint controllers arranging their relationships — Article 26 allows them to apportion responsibility for responding to such requests, and the New SCCs should enable this.
- *Specification of competent authority*. Section II, clause 9 requires the parties to specify the supervisory authority competent for ensuring compliance. This is likely to be impractical — in many cases there will not be a single supervisory authority to include in this clause. In line with EDPB guidelines,[5] data exporters carrying out cross-border processing may have multiple lead supervisory authorities for different processing operations, or may not have a lead authority; and
- *Jurisdiction of Member State courts*. Section III, Clause 3 requires the parties to submit to the jurisdiction of the courts of a specified EU Member State. Further, the Clause does not allow recourse to arbitration, which is common in commercial agreements. At a minimum, the choice of forum should be left to the parties, to avoid overlapping dispute resolution procedures in courts (for data protection matters) and arbitral tribunals (for other contractual matters) arising from the same event.

2. Revoking the Current SCCs only a year after the New SCCs come into effect is too soon

Clause 3 of the draft Commission Decision related to the New SCCs allows organizations to rely on the Current SCCs for one year after the New SCCs come into force. Updating the SCCs will require some time for the multiple contractual (re)negotiations that will need to take place between parties currently using SCCs.

We recommend that the Commission grants a substantially longer transition period for companies to move to the New SCCs, or even allows companies to continue to rely on the Current SCCs either indefinitely (while requiring use of the New SCCs for new contractual arrangements) or gradually as

[5] *See* WP 244 rev.01, pp. 5-6, 8.

contracts are being reviewed and updated. The CJEU found in *Schrems II* that the Current SCCs continue to provide adequate safeguards for transfers of personal data outside the EEA, subject to additional safeguards that the parties put in place. As a result, the Current SCCs thus could remain in place as a valid transfer mechanism for longer than a year provided that the additional safeguards are adopted where required.

3. Requirements for data exporters to notify the supervisory authority if the laws affecting importers change go beyond the requirements of the GDPR and *Schrems II*

The New SCCs require the exporter and importer to document their assessment of whether the SCCs provide appropriate safeguards. In doing so, they must take into account, among other considerations, the laws of the recipient country and practical experience of transfers to that country (Section II, Clause 2(b)). Allowing companies to take into account past experience of government requests for data, or a lack thereof, is an important element of this analysis, and it is positive that the new SCCs refer to this factor directly. The GDPR requires companies to assess the practical risks to data subjects, not theoretical or remote risks; companies' actual experience of government requests for or access to data is a vital part of this sort of assessment. This is also in line with the CJEU's holding in *Schrems II* and should therefore be reflected in the New SCCs as well as in practice.

However, we note that in addition to this *a priori* assessment, if an importer becomes subject to laws that change these assessments, the exporter must decide whether to continue with the transfer, and must inform the competent supervisory authority of the situation in that case—including where the exporter identifies and adopts additional safeguards to address any deficiencies (Section II, clause 2(f)). This broad notice obligation should be removed from the final version of the New SCCs. This notice obligation should refer explicitly to a change that causes the importer to believe "it can no longer fulfil its obligations under the Clauses."

Requiring this sort of notice in such cases goes beyond what is required by the GDPR. The GDPR permits international transfers where the "controller or processor" has provided appropriate safeguards for personal data — and GDPR Art. 46(2) specifically states that transfers pursuant to SCCs may take place "without requiring any specific authorisation from a supervisory authority." The CJEU's decision in *Schrems II* also supports this view. The Court found that "in the absence of a Commission adequacy decision, it is for the controller or processor established in the European Union to provide, inter alia, appropriate safeguards" (*Schrems II*, para. 131). More generally, the GDPR's accountability principle is designed to ensure controllers and processors take appropriate decisions related to processing, including in relation to international transfers, and requires consultation with supervisory authorities prior to processing only in scenarios that would be high-risk in the absence of measures taken to mitigate that risk (GDPR Art. 36(1)). In any event, the GDPR would require the exporter to carry out a prior consultation with the supervisory authority if the exporter concluded that the transfer met the Article 36(1) threshold.

4. The obligations on data importers that receive requests from government authorities should reflect common privacy-protective practices

We suggest refining aspects of the obligations regarding government access requests, to better reflect the circumstances under which data importers should notify and challenge requests. For example, clause 3.2(a) requires the data importer to "exhaust all available remedies to challenge" a request if there "are grounds under the laws of the country of destination to do so." Read broadly, this could require data importers to challenge requests even where there is no realistic possibility, or no possibility at all, of success, on the basis that "grounds" for challenge are, in principle, "available." The New SCCs should revise the language about exhausting "all available" remedies to clarify that they require importers to request waivers of notice prohibitions and to challenge government requests only where, on a careful assessment of the request and the laws of the country in question, there are reasonable grounds for doing so.

In addition, clause 3.2(a)(i) addresses notification in scenarios where the data importer is not prohibited from notifying the data exporter and/or data subject about this request. In that scenario, clause 3.2(a)(i) sets out information to be included in that notice. We recommend modifying this language, to provide that such notification shall include "*insofar as possible*" the information set out in that clause, including information about the personal data requested, the requesting authority, the legal basis for the request, and the response provided. This will provide more flexibility for data importers to provide notice, even if they may be prohibited from providing certain aspects of the information to be included in the notice.

5. Data importers should only accept instructions from the data exporter

Clause 1.1 of the P-P module requires data importers to accept instructions from both the data exporter and the controller. This could create a situation where a processor must accept instructions directly from a controller with whom the processor has no relationship. Requiring a sub-processor to respond to instructions from a controller they do not know and cannot verify, upends the protections of that processor and creates security implications that could be severe. To maintain adequate security and privacy protections, data importers acting as subprocessors should only be required to accept documented instructions from a controller, as reflected in the instructions provided to that subprocessor by the data exporter.

Additionally, the requirement under clause 1.1 to make available a full list of controllers creates a risk of exposure to potentially sensitive trade secrets, particularly when a company may act as a processor for many controllers in the course of the same service. Further, controllers would not even have a say in whether their identity as a customer of the processor exporter is exposed. In many cases, processors and subprocessors may store data in privacy-protective ways that prevents the subprocessor from looking at it except in limited circumstances in line with instructions from a controller; these may allow the subprocessor to safeguard the data by processing it in line with the processor's instructions without needing to know the identity of the underlying controllers. At a minimum, clause 1.1 should instead require a category list.

6. Several aspects of the audit requirements need clarification

The new SCCs contain several documentation and compliance requirements related to audits as well as determinations of which parties may require an audit. We would welcome clarification under clause 1.9(c) of the C-P module if it is indeed the data exporter's choice to require either an audit or review. To the extent it is the data exporter's choice if an audit takes place, we recommend clarifying the language in clause 1.9(d) of the C-P module and clause 1.9(d) of the P-P module by including an entry that states, "In the event of an audit…" Additionally, it is unclear whether the second sentence under clause 1.9(d) of both the C-P and P-P module intends to say "data exporter" instead of "data importer" as the language currently reads.

Similar to the concerns raised above in section 5 (with regard to clause 1.1), clause 1.9 of the P-P module creates a concern by requiring a data importer to respond to inquiries and provide sensitive compliance information to a controller with whom the processor has no relationship and that it cannot verify. That result creates several concerns, including effectively making audit data public by providing it to unknown controllers, and leaving data importers with few if any ways to protect against potential competitor audits. As such, we recommend restricting public access to sensitive audit information.

7. **The draft New SCCs appear to require a data importer to accept the decisions of competent EU supervisory authorities and courts, even if it has not exhausted its ability to seek review of those decisions**

Under the New SCCs, where a data subject invokes a third-party beneficiary right against an importer (except in a processor-controller scenario), the importer must abide by decisions that are binding under applicable laws, and must comply with measures adopted by the competent supervisory authority in relation to the transfer (*e.g.*, orders to cease processing or take action to come into compliance) (Section II, clauses 6(d), 9). We welcome this commitment as a mechanism for ensuring that EU data subjects have a right to redress in the event of a breach by the data importer. However, the current drafting could be read to require compliance regardless of the possibility of appeal from such binding decisions or supervisory authorities' measures, even where the data importer considers it is appropriate and lawful to appeal. The New SCCs should only require data importers to abide by these decisions or measures insofar as they choose not to exercise any right to appeal or all avenues for an appeal have been exhausted.

8. **The New SCCs should allow controller-importers to provide information about categories of recipients in the same way that the GDPR does**

The New SCCs place an onerous obligation on controller-importers to provide data subjects with information about the identities of all third party to which it intends to disclose their personal data (Section II, module 1 (controller-controller), clause 1.2(a)(iii)). Making identities publicly available can be extremely difficult for companies to operationalize, and it could also lead to vendor lock-in if a company is unable to use data already collected if they subsequently change individual vendors. This is a stricter obligation than is placed on controllers in the GDPR, which allows them to describe either the recipients or categories of recipients (GDPR, Arts. 13(1)(e) and 14(1)(e)). We encourage the Commission to follow this standard in the new SCCs, focused on the *categories* of third parties rather than the identity of each third party, rather than imposing a new and higher one.

For further information, please contact:
Thomas Boué
Director General, Policy – EMEA
thomasb@bsa.org