Computer & Communications Industry Association
Tech Advocacy Since 1972

CCIA comments on the draft SCC implementing decision

CCIA welcomes the timely publication of the draft Standard Contractual Clauses ('SCC') implementing decision. We generally support the current draft and believe it will pave the way towards greater legal certainty for most data transfers outside the European Economic Area. However, we are concerned that some aspects of the draft implementing decision and the draft Clauses are impractical, while others go beyond the CJEU Schrems II decision and the GDPR.

Executive summary

CCIA welcomes the timely publication of this draft decision and believes it will pave the way towards greater legal certainty for the vast majority of data transfers outside the EEA.

We are pleased to see that the draft decision addresses some of CCIA's earlier comments[1] and explicitly allows service providers that are not established in the Union to use Standard Contractual Clauses (Recital 7). The draft decision also introduces helpful improvements to facilitate the use of SCC globally, including coverage and easy to use contract modules for all-four transfer scenarios (C2C, C2P, P2P, P2C).

CCIA commends the European Commission for adopting a sensible, risk-based approach for situations where a data importer is subject to foreign data disclosure laws but has never received, and/or is unlikely to receive, any disclosure requests that would be relevant for the type of data transferred (Section II, Clause 2(b)(i)). This is a helpful clarification which reflects both the General Data Protection Regulation's emphasis on identifying and mitigating "likely" risks (not theoretical risks), the findings of the CJEU in its *Schrems II* decision.

However, CCIA is concerned that some aspects of the draft implementing decision and the draft Clauses are either impractical or appear to exceed the requirements established by the CJEU Schrems II decision and the GDPR. Specifically:

1. **Transition period:** under Article 6(3), it is unclear whether organisations contracting with new customers after the entry into force of the new SCC would benefit from the one-year transition period, and what a "change" of contract means. A one-year transition period will not be enough time for many businesses which rely on thousands of contracts with different parties. Considering that the CJEU upheld the current SCC implementing decision, the European Commission may wish to consider introducing some flexibility for parties which are currently using or will use updated SCCs.

[1] CCIA response on the review of the application of the General Data Protection Regulation, 26 May 2020, page 3, available on https://www.ccianet.org/wp-content/uploads/2020/05/090166e5cea823cc-2.pdf

2. **Suspensive effect of a transfer suspension/ban decision:** Section II, Clause 6(d) should be clarified to only require the data importer to immediately suspend transfers pursuant to a Supervisory Authority decision if it chooses not to appeal or if all avenues for an appeal have been exhausted.

3. **Challenging government data requests when it makes sense:** Section II, Clause 3(3.2) should clarify that data importers should challenge conflicting third-country data access requests where there is a realistic chance of success.

4. **Consistency between processing agreements and SCC:** Modules 2 and 3 should be consistent with Article 28 GDPR to avoid confusion and possible renegotiations of existing processing agreements that would further delay the implementation of the new SCC.

5. **Meaningful transparency:** It should be clear in Recitals 4 and 11 of the draft implementing decision that data subjects may receive a copy of the SCC upon request, consistent with the Clauses in the Annex.

6. **Realistic provision for processor-processor module:** Processor-processor SCC should only govern relationships between processors and sub-processors. Sub-processors should not have to interact with controllers or data subjects in P2P transfers.

7. **Module identification and SCC implementation for parties with multiple roles:** It should clarify how exporters and importers should sign SCC where one of the parties mainly act as a processor but also qualify as a controller for any value-added services it may provide its client.

Finally, CCIA invites the European Commission to consider providing **country-to-country guidance on foreign laws and practices which do not "respect the essence of the fundamental rights and freedoms, [...] exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) GDPR [and] contradict the Clauses."**[2] Such guidance would be of significant value to companies in scrutinising their own data transfers to these jurisdictions.

You will find CCIA's detailed comments further below.

[2] Section II, Clause 2(b)(i)

1. A meaningful and more flexible transition period

Article 6(3) requires all organisations that are already using SCCs to switch to the new SCC within one year after the adoption of the draft implementing decision, "provided that the contract remains unchanged."

First, it is unclear whether organisations contracting with new customers after the entry into force of the new SCC would also benefit from the transition period, or must implement the new SCC from Day 1, with no advance notice.

Second, while a one-year transition period may suffice for organisations with limited contracting parties and transferring a small volume of personal data, this may not be enough time for digital native organisations that rely on thousands of contracts to transfer data to their customers, vendors, and/or third parties. CCIA draws attention to the fact that all parties need time to review, implement at the technical and organisational levels, and sign SCC and any additional contractual arrangements. The more parties involved, the longer it will take for each organisation to complete their transition to new SCCs.

In addition, we note in section 4 of this paper that the New SCC deviates from Article 28(3) and (4) GDPR in several counts e.g., personal data breach notifications, audits, accuracy, etc. In many cases, any inconsistencies between the SCC and the GDPR will necessarily affect existing processing agreements, risking further delay for parties to implement and sign new SCC that is consistent with the wider processing agreement(s).

Finally, Article 6(3) implies that the New SCC should be implemented from Day 1 as soon as a contract has been updated. It is unclear whether the "change" of contract refers to a change of data processing instructions, a change of the commercial offer, and/or any other change.

Considering that the CJEU confirmed the validity of Decision 2016/2297, the European Commission may wish to extend the transition period for anyone looking to use the New SCC - whether when updating existing SCC or when setting up the first SCC as part of a new contractual relationship.

In addition, or alternatively, the European Commission may wish to consider introducing some flexibility on a case-by-case basis for organisations which rely on thousands of existing SCCs. For instance, a Supervisory Authority may extend the transition period if an organisation has already updated its existing SCC in light of the Schrems II decision (i.e., with a data transfer impact assessment, and the introduction supplementary measures) and/or if it is able to demonstrate that it has engaged with a party who proves unresponsive.

2. Data transfer suspension or ban should be effective as soon as all appeals have been exhausted or waived

Section II, Clause 6(d) appears to allow the possibility of a data transfer suspension or ban as soon as a Supervisory Authority has adopted a decision regardless of whether the parties intend to or have appealed the decision.

A decision to suspend or ban data transfers can have significant adverse effects on the parties, their customers and their vendors as the case may be. As a rule, CCIA believes that any decision by a Supervisory Authority should be effective as soon as the parties have exhausted all avenues of appeal, or if they have waived their right to appeal the decision.

There may be limited exceptions to this rule, such as in case of gross negligence of the data importers and/or data exporters. This may be the case where the data importer and the data exporter did not take any steps to review their data transfer impact assessment and implement the relevant supplementary measures, or where the parties fail to cooperate with the Supervisory Authority during the investigatory stage.

3. Data importers should challenge conflicting third-country data access requests where there is a realistic chance of success

CCIA supports provisions which oblige data importers to do their utmost to challenge third country data access requests that do not comply with the terms of their SCC and/or the GDPR.

However, a duty to "exhaust all available remedies to challenge" any third country request simply because there "are grounds under the laws of the country of destination to do so" (Section II, Clause 3.2(a)), regardless of any realistic chance of success under foreign laws, would stack up legal costs onto data recipients with little to no benefits for data subjects. We invite the European Commission to amend the SCC and clarify that they require importers to challenge government requests only where, on a careful assessment of the request and the laws of the country in question, it would be reasonable to do so.

CCIA also invites the European Commission to clarify that the legality review of the data access request by the data importer should consider the existence of any bilateral or multilateral agreement on government data access fulfilling Article 48 GDPR, and whether the request, and transfer thereof, is "necessary for important reasons of public interest *recognised* in Union law or in the law of the Member State" under Article 49(1)(d) GDPR.[3]

[3] Consistent with the European Commission's amicus brief in USA vs Microsoft, available on https://www.supremecourt.gov/DocketPDF/17/17-2/23655/20171213123137791_17-2%20ac%20European%20Commission%20for%20filing.pdf

4. Addressing inconsistencies between Modules 2 & 3 (C2P, P2P) and GDPR

Positively, the New SCC aims to embed Article 28(3) GDPR requirements. CCIA also welcomes the ability to offer certifications in lieu of on-site audits to demonstrate parties' compliance with the New SCC.

However, CCIA draws the European Commission's attention to the fact that any asymmetries between Article 28 GDPR and the New SCC (specifically Modules 2 and 3) would inevitably lead to confusion for any existing processing agreement negotiated between parties under Article 28.

CCIA is therefore concerned that the New SCC appears to deviate from Article 28 in at least four counts:

- Audits: Section I, Clause 1.9(d) and (e) provides the data exporter with a prerogative to dictate to the data importer when and how audits should be conducted, while Article 28(3)(h) and (4) leaves room for negotiations between both parties so long as audit is addressed in a processing agreement.

- Notification of personal data breaches: Section I, Modules 2 and 3, 1.6(c) extends the notification requirements of the controller (under article 33(3) GDPR) to processors, while Articles 28(3)(f) and 28(4) GDPR only mandate the data importer (processor) to "assist the [data exporter] in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing and the information available to the processor;"

- Accuracy: Section II, Clause 1.4 compels the importing processor to inform the contracting party of any inaccurate data it may have received. This obligation goes beyond Article 28(3) and (4) GDPR and it is unclear why this obligation would be necessary in the context of a transfer. Processors are unlikely to have the necessary context to determine whether data is inaccurate or out-of-date. The role of the processor should be limited to update, correct, or delete the data when instructed by the controller.

- Storage limitation: Section II, Clause 1.5 requires instantaneous deletion "upon" termination of the contract. This is unrealistic for complex storage systems (e.g., encrypted, and hashed dataset stored in different jurisdictions). CCIA suggests reverting to Article 28(3)(g) GDPR which requires deletion "after the end of the provision of services relating to processing".

Implementing the New SCC as is would therefore necessarily require changes to existing processing agreements under Article 28, risking further delay for parties to implement and sign the new SCC.

To avoid any misinterpretation and conflicts, CCIA recommends that these clauses are amended to reflect the GDPR.

5. Meaningful transparency

It should be clear in Recitals 4 and 11 of the draft implementing decision that data subjects may receive a copy of the SCC upon request, consistent with the relevant Transparency Clauses in the Annex, namely Section II Clause 1(Module 1)(1.2)(c), (Module 2)(1.3), and (Module 3)(1.3). We believe this point is just a matter of consistency.

We believe that the parties should be able to provide this information to the data subject in different ways, depending on the relationship between one or both parties with the data subject and the service(s) provided to the data subject. For instance, it may be more suitable in some cases to provide a copy of the SCC after a request by email or by filling out an access form, and in other cases, provide that information on a dedicated webpage in the privacy policy or a privacy dashboard.

6. Processor-processor SCC should only govern relationships between processors and sub-processors

Section I, Clause 1(b)(ii), Clauses specific to module 3, and Annex IA ("list of parties") appear to create an artificial relationship between a controller and a sub-processor in the context of P2P SCC. Additionally, Section II, Clause 3(3.1)(a) directs a sub-processor to notify the data subject of any third country government data access requests. This creates a direct relationship between a sub-processor and the data subject.

In practice, sub-processors such as hosting providers (sub-processor) do not, and cannot, be aware of, and manage a direct relationship with the significant number of end-users (controllers) using a provider of an online application (processor). The same is true for data subjects whose personal data are processed according to the instructions of the end-user (controller) that the SaaS service provider (processor) has forward to the IaaS service provider (sub-processor).

Take for example an online conference software provider (controller), serving millions of business customers and consumers, whose service is hosted by a hosting service provider established in the EU (processor) which transfers data to a subsidiary outside the EEA for operational purposes (sub-processor). In practice, the online conference software provider only provides processing instructions to its hosting provider, and the latter's subsidiary has no way of knowing the identity of the online conference software provider, let alone the customers of the hosting provider.

While CCIA agrees that the sub-processor should process personal data in accordance with the instructions of the controller, the controller should not be involved in a processor-processor relationship. It should be clear that it is the sole responsibility of the processor (data exporter) to give the sub-processor (data importer) further instructions that the controller may have

requested from the processor (data exporter). Similarly, it is undesirable from the perspectives of both the data subject and the data sub-processor to be able to directly interact with one another.

Given the existing rights for data subjects under GDPR to enforce rights against sub-processors, sub-processors should not have to interact with controllers or data subjects in P2P transfers.

7. Identification and implementation of modules for organisations performing multiple roles

From a practical perspective, it is unclear how data exporters and data importers should sign SCC where, for instance, one of the parties act mainly as a processor but also qualifies as a controller for any value-added services to its client.

To dissipate any confusion, CCIA encourages the European Commission to clarify whether different modules and versions of Annex I.B can be combined in a single set of SCC or whether parties should enter into separate SCCs for each transfer.

8. Non-binding guidance on third-country laws to ensure the smooth implementation of the new SCC

Consistent with the Schrems II decision, the draft SCC compels parties to assess whether the laws of the country where personal data is transferred "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 of the objectives listed in Article 23(1) GDPR", and "are not in contradiction with the Clauses" (Section II, Clause 2(a)).

While we do not dispute this obligation, CCIA draws attention to the fact that this type of assessment is costly, time consuming, and requires a depth of knowledge which most companies do not have. Most companies are not, and will never be, in a position to identify and assess which laws in the country(ies) of destination would fail to meet the EU's proportionality and necessity test, particularly as the case-law evolves. These assessments will also pose an unrealistic burden for public bodies and other organizations working in the public interest, such as research institutions.

For companies that cannot afford external counsel from multi-jurisdictional legal specialists, conducting this assessment on an individual basis would inevitably lead to different findings for the same jurisdictions. Compliance fragmentation would be further aggravated if counsel relies on an incomplete EDPB assessment of U.S. laws and practices and a partial outline of the the recent CJEU case-law on serious interferences with individuals' rights in the context of national security, such as is the case in Recommendations 01/2020 and 02/2020.

As we have pointed out before,[4] CCIA believes that the European Commission, in consultation with the EDPB, has a crucial role to play and should issue non-binding guidance on third-country laws and practices of concerns. This guidance could help companies identify and further scrutinise their own data transfers to these jurisdictions. The European Commission has the institutional credibility and the expertise in carrying out evaluations of third-country government data access laws, as is the case in the context of adequacy determinations.

To this end, we should stress that the assessment of whether the laws and practices of a given jurisdiction meet the European Essential Guarantees cannot be an individualised assessment as such. Either the laws of a third country satisfy EU requirements, or they do not. Whether a given company transfers data to countries A, B or C is irrelevant to determine whether the laws and practices of these countries (a) constitute a disproportionate interference into EU data subjects' rights, (b) are unclear, imprecise, or inaccessible, (c) do not provide an independent oversight mechanism, (d) do not effective remedies for EU data subjects.

Furthermore, nothing in the General Data Protection Regulation, the CJEU Schrems II ruling, or the existing or future Standard Contractual Clauses, would prevent the European Commission, working alongside the EDPB, to publish non-binding essential equivalence guidance. While the CJEU reminded that it is the responsibility of the data exporter to ensure that EU data protection travels with the data, the CJEU does not prohibit the Commission or the EDPB to assist data exporters in this endeavour.

CCIA is all too aware of the herculean task that assessing the laws of 152 non-adequate jurisdictions would involve. That is why we kindly suggest first focusing at least on the EU's largest trading partners, including updated information from the United States, the United Kingdom, China, India, South Korea, Russia, Turkey, Mexico, Brazil, etc.

CCIA strongly believes that a uniform country-level guidance would significantly help companies throughout their self-assessment journey.

CCIA stands ready to further assist the European Commission in their endeavour to provide much needed clarity for European and international businesses doing business in the EU.

***

For further information, please contact:
Alexandre Roure, Senior Manager, Public Policy, CCIA Europe: aroure@ccianet.org
Keir Lamont, Policy Counsel, CCIA: klamont@ccianet.org

[4] CCIA's paper on Ensuring Secure Data Transfers post 'Schrems II', sent to the European Commission on 27 October 2020, and available on https://www.ccianet.org/wp-content/uploads/2020/10/2020-10-27-CCIA-Comments-to-European-Commission-and-EDPB-on-Ensuring-Data-Transfers-post-Schrems-II.pdf