Standard Data Protection Clauses EC draft (Nov 2020): Comments on public consultation

Feedback on the standard data protection clauses for transferring personal data to non-EU countries (implementing act)

December 2020

Table of Contents

1 About the authors

Self-Regulation Information Economy (German: Selbstregulierung Informationswirtschaft e.V. – short: **SRIW**) is a Berlin-based non-profit-organization that fosters and promotes data and consumer protection through self-regulation and co-regulation and acts as a monitoring body for data protection codes of conduct. Its Brussels-based subsidiary SCOPE Europe sprl / bvba (**SCOPE Europe**) complements the portfolio of **SRIW** on a European level and is in the process of acquiring to become an accredited monitoring body under the European General Data Protection Regulation (GDPR), pursuant to Article 41 GDPR. **SCOPE Europe** acts as monitoring body for the EU Data Protection Code of Conduct for Cloud Service Providers (short: **EU Cloud Code of Conduct**).

Standard data protection clauses (SDPC) according to Art. 46 (1) GDPR had been absent during the GDPR's lifespan so far. As a result, SRIW, SCOPE Europe, and a consortium of different European and international companies developed a draft set of clauses as a self-regulatory guidance initiative, introducing key principles and safeguards for the processor to processor environment. The development of these clauses was driven by the need for an as comprehensive and accurate regime as possible, while safeguarding a high level of data protection for third country transfers. At the same time, it was ensured that particularly small and medium-sized companies could rely on such clauses.[1] The initial publication of the draft clauses took place in June 2019. The latest version is version 2.4, published in May 2020 ("**our SDPC draft**").

SRIW and SCOPE Europe welcome that the European Commission has now published its draft SDPC and has invited stakeholders to submit comments during the public consultation phase. The Commission's guidance will prove important for the further growth of SDPCs as an important tool. As we worked on our "own" set of Clauses as described above, we were able to gather many relevant market insights and developed some possible solutions for a comprehensive framework which we would like to bring in as part of this public consultation, as we did to the extent possible already in coordination with the European Commission.

In addition, these comments that reflect the gathered expertise specialised in the development and monitoring of codes of conduct based on Articles 40-41 GDPR, specifically our role in the EU Cloud Code of Conduct. The latter pays great attention to data transfers to third countries, and we are

[1] All details on that project, including the Clauses as such and a dedicated explanatory document, can be found here: https://scope-europe.eu/en/projects/standard-data-protection-clauses/ The development of this project is currently supported by Alibaba Cloud (Singapore) Private Limited, DATEV eG, Fabasoft AG and SAP Belgium NV/SA.

currently developing a third country transfer 'add-on module' to the Code to help stakeholders gain additional legal certainty. Also, in this context, the European Commission's updated draft SDPC ("**EC SDPC 2020**") are of utmost importance.

As a result, we are pleased to share our comments in the following, which are highly focused on our expertise within the ecosphere of third country transfers. Our comments should be read in this light, and notwithstanding broader comments by other stakeholders.

2 Executive summary

We appreciate the chance to provide comments on the new standard data protection clauses for the transfer of personal data to third countries pursuant to Article 46 GDPR. We acknowledge the great value of the updated framework, which will help companies when relying on third country transfers.

- We appreciate the efforts undertaken by the European Commission in modernizing the SDPC framework, also to reflect the Schrems II judgment. In particular, we welcome the introduction of the new Clauses also for the processor-to-processor environment.
- From our perspective, there are several areas where the updated clauses can be further improved, such as the terminology used, questions of enforceability and some provisions that seem to be phrased ambiguously. We also noted that some concepts may be subject to different interpretations or even misunderstanding by the parties actually implementing the Clauses, e.g. in relation to the so-called docking clause.
- However, it is also worth stressing that we welcome many provisions which can enable companies to implement a robust framework for third country data transfers, especially the mentioned sections which follow a similar approach to our SDPC draft.

We hope our detailed comments may contribute to the further enhancement of the SDPC and we look forward to further contributing to the related developments.

3 Introductory remarks

We would like to thank the European Commission for granting stakeholders in the field the opportunity to issue comments on new regulatory documents, while simultaneously greatly appreciating that our comments have been taken into account in the past. Finally, we agree with the EU's 'Better Regulation' strategy that consultations are not only an important element to achieve a higher quality of regulation, but also help achieve a broad base of support among the regulated.

4 Remarks and observations

4.1 A high-quality draft with many sensible provisions

First, we appreciate the overall quality of this draft document. Many provisions appear well-considered, such as the notification requirements, and **we welcome in particular that many provisions seem to follow a similar approach to our SDPC draft** (for example Section II Clause 2 e EC SDPC 2020 and Section II Clauses 6 – 9 EC SDPC 2020 in relation to Clause 4.7. b of our SDPC draft). We are also pleased that the possibility has been maintained to **integrate the clauses in a broader contractual framework**, which is imperative for stakeholders that wish flexibility in their contractual relations.

We also consider 'new' requirements that were added in light of the recent Schrems II ruling, such as the obligations for the data importer to review the legality of the request for disclosure and to only share the minimum amount of information permissible, as **helpful and aligned with good practices already common in the context of Binding Corporate Rules.** By integrating such requirements, we hope that the EC SDPC 2020 will serve as a broadly accepted and adopted tool to not only offer market actors long term legal certainty, but also to boost consumer confidence in data transfers.

4.2 Clarification of certain terminology is needed

Nonetheless, we believe that EC SDPC 2020 could be further enhanced by more consistent or clear terminology.

4.2.1 "Data exporter" and "data importer" vs. generic terms such as "transferring party" "receiving party"

The **terms 'data importer' and 'data exporter' are insufficiently accurate** to capture the oftentimes complex processing chains that exist in real life, a concern we also intend to share in our public consultation comments on the EDPB's 'Recommendations 01/2020'.[2] Since the underlying idea is that the data exporter is the one transferring the personal data and the data importer is the one receiving the personal data from the data exporter, we suggest using the more generic and flexible terms 'transferring party' and 'receiving party' respectively.

While we acknowledge that the terms 'data importer' and 'data exporter' are widely used, it is worth pointing out that this mechanism is missing many common processing procedures in the market, e.g. if the 'data importer' contracts another sub-processor in the same third country. Although we are aware that this scenario shall be reflected by the newly introduced concept of "onward transfers" and we value its practical relevance, it also proves the inappropriateness of the old terms "data exporter" and "data importer". Onward transfers shall be safeguarded by the EC SDPC 2020 and, both principally and by mere application of the literal meaning, no party that is initiating an onward transfer can be a "data exporter" anymore. A more consistent approach could also be beneficial for the overall terminological cohesiveness, since the term 'data exporter' is sometimes used seemingly as a synonym for controller, or they are mentioned in close proximity without distinct obligations.

4.2.2 Definition of "data transfer"

We regret the fact that there is still **no definition of 'data transfer'**. It is highly appreciated that the urgent need of reflecting onward transfers is already incorporated. However, the legal concept of SDPCs is translating fundamental principles required by the GDPR by means of a bilateral agreement, thus applying those principles to parties that otherwise may not be subject GDPR. Keeping in mind that neither the GDPR nor the EDPB recommendations and guidelines currently attempts to define a 'data transfer', the lack of a definition may cause significant legal uncertainty that renders this SDPC ineffective. For example, at the moment important questions remain such as whether 'mere access' must be interpreted as amounting to a data transfer. Especially important is that there may be scenarios where it is necessary to have a distinct and slightly different (narrower) understanding in the context of SDPCs than under the GDPR in general.

4.2.3 "Type of recipient"

Additionally, we would like to ask for **clarification of what is meant with "type of recipient"** in Section II Clause 2 b (i) EC SDPC 2020 (page 13). Our interpretation on the "type of recipient" would be the legal role of the recipient, pursuant to applicable data protection law (e.g. controller, processor), or possibly a differentiation between public or private actors. Considering that the EC SDPC 2020

[2] Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data | European Data Protection Board (europa.eu)

inherently contains a risk-based approach, the type of recipient may in its understanding as a legal role also refer to highly relevant processing contexts (in line with professional literature and public bodies' statements of what qualifies as a "data transfer" – as well as the practical needs that were communicated to us by industry partners whilst drafting our SDPC draft).

Against this background we would appreciate if the "type of recipient" actually did allow the parties to agree upon very lean measures, especially where legal ambiguities regarding the applicability of "processing" of personal data and "data transfers" cumulate – e.g. in the context of (remote) maintenance and product support services.

4.2.4 Nature of Personal Data

We would also like to ask **clarification regarding the turn of phrase "the nature of the personal data transferred"** in Section II Clause 2 b (i) EC SDPC 2020 (page 13). A similar phrase ("Nature of the data") is also mentioned in the EDPB's Recommendations 01/2020 (para. 49). In our comments to the EDPB's recommendation we intend to highlight that a clarification is considered beneficial. Regardless, **we strongly recommend that both the EC SDPC 2020 and Recommendations 01/2020 align the terminology used** to prevent ambiguities that might limit the effectiveness of all measures being implemented.

4.3 Lack of clear enforceability

At the moment, the EC SDPC 2020 seems to lack clear provisions on the enforcement of judicial rulings. We acknowledge that the EC SDPC 2020 provide a contractual obligation to accept any judicial rulings. However, that is not an additional safeguard as it does not safeguard the data exporter's ability to enforce such rulings in case the data importer – illegitimately – refuses to comply with is contractual obligation. For inspirational purposes, we therefore kindly refer to related provisions in our SDPC draft: the Transferring Party shall assess whether there is any bilateral agreement on the enforcement of judicial rulings between a) the member state of the competent court and b) the countries of any potential enforcements against the Receiving Party.

Regarding the competent court mentioned under a), the Parties should acknowledge and agree that the court competent is the one where the Transferring Party is established. If and to the extent the Transferring Party is not established within the EU, the court competent should be the one where the representative of the Transferring Party is established. The Parties may agree to a court competent at their choice, provided that such court competent is one within the EU.

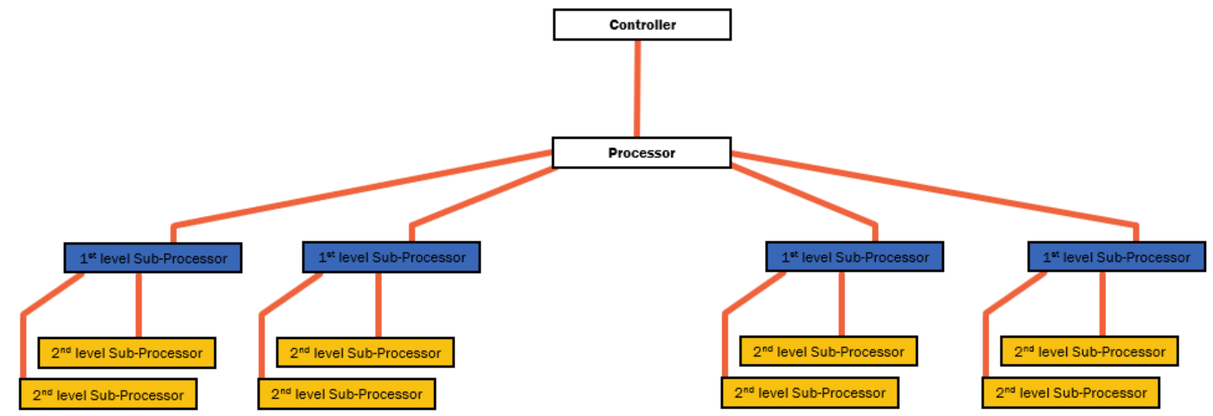
The determination of which court shall be exclusively competent regarding disputes between the Parties is very important for the sake of legal clarity. Our proposed approach intends to provide further certainty and continuity in this regard. The link to the EU furthermore ensures that an adequate application of the GDPR is safeguarded.

4.4 The docking clause raises many questions

We certainly welcome concepts that ensure the rights and obligations of all entities partaking in the actual data processing and the fact that a multi-party setting is taken into consideration. However, in the context of the so-called **'docking clause'** as introduced in Section I Clause 6, we are struggling in understanding its overall role in and consequences for the EC SDPC 2020.

It is unclear whether this clause is optional or mandatory. Whilst the title clearly states it is optional, Section II Clause 1 Module 3 1.1 a EC SDPC 2020 creates the impression that the docking clause will be mandatory in a processor-to-processor environment if the provided conditions are met. We recommend clarifying EC SDPC 2020 by using the term "conditional" or by simply adding the provisions of the docking clause only where they are considered mandatory. We are also unsure how the docking clause would account for the right to compensation and liability pursuant to Art. 82 GDPR.

Furthermore, questions remain regarding the material consequences and intent of the docking clause. To our understanding, the docking clause intends to address the lack of third-party beneficiary rights, i.e. allowing relevant third parties to accede into an existing contract to empower them to adequately perform the rights under GDPR. If this is the case, we strongly recommend a different, more pragmatic approach that would limit bureaucratic efforts for all parties concerned and thus increase the adoption of EC SDPC 2020. It is acknowledged that not all jurisdictions provide the concept of third-party beneficiary rights, but many jurisdictions that do. Instead of conceptualising the EC SDPC 2020 from a lack of third-party beneficiary rights, it should add a simple condition: an obligation to verify the applicability of such a concept to the governing law. By that, a mere formalistic administrative burden to seek individual signatures by each affected third party could be limited to the extent necessary (please refer to figure 1 below for an example elaborating that such a clause might create significant overhead related to managing signatures). If the parties agree to a governing law lacking third party beneficiary rights – due to other advantages of such a jurisdiction – the clause providing the concept of the docking clause can be required.



Provided there is a processing chain of only three levels (in practice, there are very often 10 levels and more), requesting each party on each level to countersign the agreement (the EC SDPC 2020) concludes as follows. The controller engages a processor. The processor engages four sub-processors (1st level) and each sub-processor engages two sub-sub-processors (2nd level).

Controller perspective: The controller needs to sign one agreement with its processor, needs to countersign four sub-processing agreements (1st level), and eight sub-sub-processing agreements (2nd level); cumulating to an overall number of 13 signatures.

Processor perspective: The processor needs to sign one agreement with its controller, needs to countersign four sub-processing agreements (1st level), and eight sub-sub-processing agreements (2nd level); cumulating to an overall number of signatures of 13 (the same goes for the four sub-processors on the 1st level and the eight sub-sub-processor on the 2nd level). However, in practise, controllers and processors often work with dozens of different parties; many specialized SaaS services have thousands of controllers and thereby thousands of individual agreements. If, for the sake of this example, we would presume that the processor has 100 agreements with 100 different controllers (which is still a low estimate), there is not only a need to sign the 100 agreements per controller, but the processor also needs to receive four additional signatures per sub-processor. That amounts to 400 signatures. Provided that the signatures flow down the chain, the processor also needs to handle the signatures regarding the sub-sub-processors, which multiplies its efforts by eight. As a result, the processor needs to manage 3200 signatures. And this is only the calculation for the initial processors; the same logic would apply for each of the four sub-processors on the 1st level:

1st level sub-processor perspective: One individual sub-processor on the first level would be required to manage two signatures upwards the processing chain – one for the controller, one for the processor. Downwards the processing chain, it would be required to sign two agreements directly for the 2nd level processors. Each will require countersigning by both the controller and processor, amounting to another four agreements. Consequently, per individual customer this leads up to a total of eight signatures. As the sub-processor in our example has 100 customers (processors) this would amount to 800 signatures. Based on our example this processor itself has, 100 customers (controllers), leading to a total of 80,000 signatures that need to be managed by the 1st level sub-processor reflecting a SME, if not even micro enterprise in our example.

Respectively, the same logic would apply for each of the eight sub-sub-processors on the 2nd level (who may realistically also have 100 different agreements in other sub-processing agreements).

Yet unclear is whether the docking clause will be required to flow down and flow up the chain. Additionally, related to this provision, we recommend a clarification ensuring that the instructions of the data exporter do not contradict the instructions of the controller, or vice versa.[3]

In conclusion, while highly appreciating the need for multi-party settings, we recommend overhauling the docking clause to ensure that its administrative consequences are reduced to minimum.

[3] In our SPDC draft, we introduce a mandatory notification by the Receiving Party to the Transferring Party in case of conflicting instructions directly received by the controller.

Furthermore, we recommend specifying under which circumstances it shall apply, to guarantee legal certainty.

4.5 Certain provisions lack a clear link with third country transfers

There is a strict separation between the regulatory regimes for data transfers inside the EU (governed by article 28 GDPR) and outside the EU (governed by article 46 GDPR). However, Section II Clause 2 counts many provisions that, in our view, **lack a clear link with third country transfers** and instead lean into the general intra-EU debates on processing carried out on behalf of a controller (Article 28 GDPR). We believe the following provisions lack a clear relevance for third country transfers

- Section II Clause 1 Module 1 points 1.8 and 1.9.
- Section II Clause 1 Module 2 points 1.1 – 1.4; 1.7; 1.9.
- Section II Clause 1 Module 3 points 1.2; 1.4 – 1.7; 1.9.

We recommend rewording these provisions to distinguish them from the intra-EU context and emphasise their specific application to third country transfers.

4.6 The overall structure appears repetitive

The modular approach is highly appreciated. Completing our remark in 4.5, we believe that the overall structure of the EC SDPC 2020 could be streamlined by two aspect that appear effortless: 1) focussing on third country specific safeguards and leaving out mere repetition and/or paraphrasing of GDPR requirements 2) apply the modular structure within each clause at the very place where a distinction is needed and by that minimizing repeated language.

Related to aspect 1) we acknowledge that a certain degree of integrating general GDPR requirements is useful and necessary. Consequently, also our SDPC draft provides a few provisions of that kind. However, we recommend keeping such provisions to the very minimum possible and – to the extent possible – phrase such provisions in a way preventing potential conflicts with other contractual agreements between the parties to the best possible. We would like to refer to the following as an example, where our SDPC draft did have a potential overlap with the audit right provided under GDPR: “If and to the extent as the Sub-Processing Agreement governs modi operandi of the right to audit under Art. 28 (3) h) GDPR, such modi operandi shall prevail.”[4]

[4] Clause 2.4 our SDPC draft.

Related to aspect 2) we acknowledge that this remark certainly is also a matter of style and individual preference. However, we believe that especially SME will consider it very complicated to select the applicable provisions out of the EC SDPC 2020 being subject to lose any legal effect in case of any mistakes performed. Therefore, we recommend to integrating the modular approach directly into each provision and making certain elements conditional. For example, there could be one provision right at the beginning requesting the parties to identify the legal relationship between them. Against this, a provision might add different variations of single terms, sentences or paragraphs, respectively starting with “provided the Parties chose option Clause 1 Para 1 XYZ”. Such a conditional approach would ensure that the parties will only need to decide a very few aspects depending on their individual situation, but the rest of the EC SDPC 2020 will then work automatically.

4.7 Certain provisions seem ambiguously phrased

We believe that certain provisions are ambiguous to an extent that they may cause legal uncertainty. As a result, we suggest that the following sections are rephrased or receive extra clarification.

First, there is Section II Clause 2 Module 1 1.7 (iv) EC SDPC 2020. If a data subject has already consented to a third country transfer (with a distinct jurisdiction), a notion seems lacking in the GDPR that distinct consent is necessary for onward transfers. **The EC SDPC 2020 should be clarified that onward transfers do not require separate consent by data subjects.** Any ambiguities in this regard must be prevented as they will – in practice – make consent even less attractive and difficult to retrieve and maintain for enterprises. Already, a discrepancy exists between the concept of consent in the law, and how it is practiced. We therefore believe that this provision should be rephrased to avoid any amplification of such a discrepancy.

Second, regarding Section 2 Clause 1 Module 2 point 1.6. b. The wording that “[t]he data importer shall grant access to the data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract” seems to refer to an anchor that is incompatible with the principles and practical necessities of the GDPR. Following the Regulation, we believe the **anchor should not be the “contract” but the “processing of personal data as governed by the contract”.**

Third, regarding Section 2 Clause 1 Module 2 point 1.8. The legitimate options listed here are different as compared to C2C transfers. Instead of such individually listed legitimate options that might create confusion due to slight differences, **it is preferred to make a general reference to the mechanisms of Chapter V GDPR.**

Fourth, regarding Section 2 Clause 3 3.1 a and specifically the phrase that "[t]he data importer agrees to promptly notify the data exporter and, where possible, the data subject (if necessary with the help of the data exporter) if […]". In our understanding, **it is only the controller who is obliged to fulfil the notification duty and never the processor.** As a result, the use of 'exporter' in this context is highly ambiguous. This strengthens our belief that the terms 'transferring party' and 'receiving party' should be considered instead of 'data exporter' and 'data importer' (in line with our comments above in section 3.2.1).

Finally, regarding Section 3 Clause 1 e we are fully in favour of a derogation clause and our draft SDPC also contained a similar provision. However, we regret the fact that **this provision currently does not allow the exporter to reject prejudice of an adequacy decision**. By adding such an additional phrase, we believe more flexibility and legal certainty could be introduced.

Executive Summary

We appreciate the chance to provide comments on the new standard data protection clauses for the transfer of personal data to third countries pursuant to Article 46 GDPR. We acknowledge the great value of the updated framework, which will help companies when relying on third country transfers.

- We appreciate the efforts undertaken by the European Commission in modernizing the SDPC framework, also to reflect the Schrems II judgment. In particular, we welcome the introduction of the new Clauses also for the processor-to-processor environment.
- From our perspective, there are several areas where the updated clauses can be further improved, such as the terminology used, questions of enforceability and some provisions that seem to be phrased ambiguously. We also noted that some concepts may be subject to different interpretations or even misunderstanding by the parties actually implementing the Clauses, e.g. in relation to the so-called docking clause.
- However, it is also worth stressing that we welcome many provisions which can enable companies to implement a robust framework for third country data transfers, especially the mentioned sections which follow a similar approach to our SDPC draft.

We hope our detailed comments may contribute to the further enhancement of the SDPC and we look forward to further contributing to the related developments.

SCOPE
EUROPE

About SCOPE Europe

SCOPE Europe sprl / bvba (SCOPE Europe) is a subsidiary of SRIW. Located in Brussels, it aims to continue and complement the portfolio of SRIW in Europe and strives to become an accredited monitoring body under the European General Data Protection Regulation, pursuant to Article 41 GDPR. SCOPE Europe gathered expertise in levelling industry and data subject needs and interests to credible but also rigorous provisions and controls. SCOPE Europe also acts as monitoring body for the EU Data Protection Code of Conduct for Cloud Service Providers and is engaged in other GDPR code of conduct initiatives