noyb – European Center for Digital Rights
Goldschlagstraße 172/4/3/2
1140 Vienna, Austria

noyb's comments on the proposed Standard Contractual Clauses for the Transfer of Personal Data to Third Countries pursuant to Regulation (EU) 2016/679[1]

noyb welcomes the initiative of the Commission to update the existing Standard Contractual Clauses ("SCCs") as adopted by Decisions 2001/497/EC and 2010/87/EU, as amended. We welcome the opportunity provided by the public consultation to send the following comments on the draft decision and its annexes.

A. Equivalent level of protection for data transferred outside of the EU

The draft decision commented refers to the need to update the SCCs in light of the requirements of the GDPR, and of the important developments that took place in the digital economy.[2] An update of the SCCs was also needed in light of the recent Decision of the Court of Justice of the EU in *Schrems II*, that reaffirmed that, even if SCCs may be valid tool for transfers, additional guarantees might be required in some cases, to ensure an adequate level of protection to the data subjects.

Article 44 of the GDPR now clarifies that all provisions of Chapter V of the GDPR shall be interpreted in order to ensure that the level of protection guaranteed by the GDPR is not undermined. An essentially equivalent level of protection must therefore be guaranteed irrespective of the provision of that chapter on the basis of which a transfer of personal data to a third country is carried out.[3] On this basis, all transfer instruments (*e.g.* BCRs, SCCs, derogations) should lead to an essentially equivalent level of protection when compared to the GDPR.

It follows that all principles of the GDPR and all rights for the data subjects must be reflected in any transfer instrument. The rights granted to the data subjects cannot be lower under the SCCs than e.g. under an adequacy decision – which some have previously argued. The SCCs function to fill any vacuum in the laws of a third country – and must do so fully and in all respects.

In this context, we could identify the following points in MODULE 1 (controller to controller) where the rights and principles of the GDPR are lacking entirely or partially (this list is not exhaustive):

- the right to object is limited to direct marketing
- the right to withdraw consent is not mentioned
- the right to data portability is not made available to the data subjects
- the right no to be subject to automated decision-making is not fully implemented[4]
- the SCCs do not refer to the right to restriction of processing.

---

[1] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12741-Commission-Implementing-Decision-on-standard-contractual-clauses-for-the-transfer-of-personal-data-to-third-countries.
[2] See Recital 6 of the Draft decision.
[3] *Schrems II*, § 94.
[4] Contesting is not the same as the "right not to be subject". Moreover, the wording of the relevant clause is not in line with the GDPR: see table below.

We therefore suggest to ensure all principles of the GDPR are included in the SCCs to avoid that any controller or processor may interpret them in a way that the level of protection provided by the GDPR is undermined when personal data are transferred outside of the EU.

B. Highly Complexity System

As a general feedback, we would like to highlight that the draft decision is very complex and that the various modules are not easy to comprehend at first sight. While we welcome that the proposal covers many more transfer situations, we would suggest to split the various scenarios into separate instruments or annexes to allow less experienced controllers and processors to correctly implement this decision. Equally, a "text generator" or some similar tool may be useful for controllers and processors that do not employ an expert data protection lawyer. We fear that the current version may lead to many errors in real-life implementations.

C. Assessment of the laws of the third country based on the specific circumstances of the transfer

The draft implementing decision requires organisations to take into account the specific circumstances of a transfer, such as the content and duration of the contract, the nature of the data transferred, the type of recipient, the purpose of the processing and any relevant practical experience indicating the existence or absence of prior instances of requests for disclosure from public authorities received by the data importer for the type of data transferred.[5]

This wording seems to interpreted by some controllers and processors as meaning that even when there are third country laws that violate the GDPR this can be ignored when these laws were not used , or not used enough by a third country government. In essence this would lead to a "law *or* practice" approach where either the law or the subjective practice is compliant with EU law. This approach was pleaded in *Schrems II* and rejected by the CJEU. The EDPB equally rejected this idea and instead highlighted that organisations should rely on objective factors when assessing the impact of the law *and* practices in the data importer's jurisdiction on the effectiveness of the safeguards provided in the SCCs.[6] In other words: There needs to be a proportionate law and third countries must follow these laws in practice.

From a practical perspective, taking into account relevant practical experiences indicating the existence or absence of prior instances of requests for disclosure would be extremely difficult since access by public authorities is usually confidential and such an element is wholly a matter of the controller or processor to prove. In practice most representatives of an organisation will also not know about secret surveillance within their own organisation and therefor by definition take the (subjectively correct) view that there is no such surveillance. It is therefore almost impossible for a supervisory authorits and even less any data subjects to know that such access took place in the past and to invoke their rights under the SCCs.

Moreover a subjective approach usually leads to very different results for different data subjects. By definition most access only concerns a small subset of users (e.g. journalists, activists, politicians, high level business persons, dissidents, persons of certain religious beliefs and alike). In such cases, any assessment that is based on the general population is usually incorrect for the specific data subject.

Finally, the law of the third country should be easy to understand and interpret for the data importer and the data exporter, in order to determine whether the data are subject to surveillance laws. Should this not be the case, one should draw the conclusion that the law in the third country does not meet the standard of accessibility and transparency required under EU law. [7]

---

[5] See Section II, Clause 2 (b) (i) of the SCCs, and Recitals 19 and 20 of the draft decision.

[6] Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, adopted on 10 November 2020.

[7] We refer in this respect to the EDPB's Recommendation 02/2020 on the European Essential Guarantees for

We are also concerned to see an increasing number of papers and statements suggesting that transfers should be assessed on a case-by-case basis, following a "risk-based approach". However, such an approach is not a general principle applicable to all provisions of the GDPR. Like in many other texts, the EU legislators adapted the obligations and requirement of the GDPR on the basis of the risk for the individuals. This is the case in the following instances:

- assessment of the compatibility of a further processing taking into account the possible consequences thereof for the data subjects (Article 6(4) (d) GDPR)
- assessment of the security measures of a specific processing (Article 32(1) GDPR)
- assessment of the risks for individuals in case of a data breach (Articles 33(1) and 34(1) GDPR)
- data protection impact assessment and assessment of potential high risks to the rights and freedoms of individuals (Articles 35 and 36 GDPR).

Nothing in Article 46(1) or 46(1)(c) indicates that a transfer my take place when it presents a low risk (risk of interception by a public authority for example), or that it would require a so-called "transfer impact assessment". Therefore, we invite the Commission to revise the relevant clauses to reflect the remark here above, in particular Clause 2(b) and any related recitals.

In any event, *noyb* will closely monitor the developments regarding this point and take appropriate legal steps should the Commission adopt such an approach and controllers actually rely on this approach.

D. Practical help with assessments

While others may be better placed to comment on this issues, we would like to recognize that most smaller organisations will be unable to conduct a proper assessment of the laws of a third country. Such an assessment is highly complex and requires cross-jurisdictional expertise. Usually experts for (partly very exotic) other jurisdictions are not available in most Member States and local experts in the given third country are not aware of the requirements under the SCCs, GDPR and CFR.

We would therefore encourage the Commission to think about ways to provide such assessments for the most important trading partners of the Union, be it via the EDPB, SAs or via independent researchers. A relatively small investment in such publicly available assessments may ensure that these assessments are accurate but also realistically available to smaller organisations.

E. Territorial scope – definition of transfer

We note that the GDPR does not define a "transfer" within the meaning of Article 44 GDPR. Two interpretations are currently floated: a geographical approach and a jurisdictional approach. *noyb* does not take a position on this question, as further research seems to be necessary to take a position. Initial research suggests that the approach jurisdictional approach is rather novel and far from mainstream.

Recital 7 of the draft decision states that the SCCs may be used for transfers of personal data "*to a processor or a controller established in a third country*". The Recital adds that "*this also includes the transfer of personal data by a controller or processor not established in the Union, to the extent that the processing is subject to Regulation (EU) 2016/679 pursuant to Article 3(2) thereof*".

---

surveillance measures, and in particular to the first condition, that is that a justifiable interference (including access to data by public authorities) must be based on clear, precise and accessible rules.

Article 1.1 of the draft decision states that the SCCs will be considered as appropriate safeguards within the meaning of Article 46(1) GDPR when the exporter is subject to the GDPR and when the importer is not subject to the GDPR.

Jurisdictional Approach

In our understanding of the draft, the Commission seems to consider that one can only speak of a "transfer" of personal data under the GDPR when the importer is not subject to the GDPR. In this case where both the data exporter and the data importer are subject to the GDPR, and the latter is based outside of the EU, no adequate safeguards (and therefore no SCCs) would be required under Chapter V of the GDPR, since no "transfer" takes place.

Such an interpretation may create substantial loopholes and inconsistencies in the GDPR and the protection of data when a transfer occurs. Some examples:

- There seems to be no practical way that e.g. an EU SAs would be able to exercise the powers under Article 58 GDPR or enforce a fine under Article 83 or 84 in a foreign territory. So far this was overcome by the contractual arrangement in the SCCs where controllers voluntarily accept the SAs powers in any third country. We fail to see any other way that a SA could use to e.g. perform on-premises investigations in a third country without voluntary acceptance in a contract.
- The obligation to appoint a representative in the EU is not a guarantee of enforceability of the GDPR. Many companies simply never appointed a representative - for example because they may be of the incorrect view that the GDPR does not apply to them. These representatives often neither have the relevant information to assist an investigation nor relevant assets or decision powers to provide for an effective avenue for enforcement.
- Equally, in the absence of any voluntary choice of law and jurisdiction clause in a contractual arrangement, any decision may not be recognized by a third country and therefore not be enforceable by the data subjects.
- Further to that, Article 3(2) GDPR already applies when the processing "*relates*" to the "*offering of good or services*" in the Union. This would potentially make a lot of organisations subject to the GDPR, considering that most transfers relate in some way to the offering of goods and services in the Union. The practical scope for Chapter 5 of the GDPR would therefore be almost non-existent. We are not sure if this approach is systematically correct.
- Because of these issues, some SAs currently do not even investigate cases where a controller subject to the GDPR is not based in the EU, considering that they lack competence to investigate the case and/or enforce their decision. The lack of any voluntary acceptance of EU jurisdiction in a contractual arrangement may further add to his problem.

We would also like to highlight that the CJEU has not taken a "jurisdictional approach" in C-311/18 - *Schrems II*, despite the fact that the GDPR was applied and the relevant transfer was clearly "related" to the offering of a service to an EU data subject.

Considering the above, while the approach undoubtedly has some elegance to it, the lack of any voluntary acceptance of European jurisdiction by a third country entity may make the GDPR in practice less enforceable than under the current approach. The ever-expanding claims of direct EU jurisdiction may end up to be a one-sided claim that overstretches the boundaries of international law.

Uniform view on "transfer" required

In either case, a common understanding of the word "transfer" under the GDPR would solve the problem. In such circumstances, we urge the EDPB to provide its interpretation of what is considered a transfer under the GDPR, as we think that it is not the competence of the Commission to do so, especially in an implementing decision.

Without any such common view on the meaning of a "transfer" the Commission may risk that the CJEU would invalidate the entire new SCC system.

E. Interaction with the SCCs adopted by the Commission on the basis of Article 28(7) GDPR

We also welcome the draft decision of the Commission suggesting model clauses on the basis of Article 28(7) GDPR ("Article 28 SCCs"). As stated above, whereas the transfer SCCs apply to a controller or processor subject to Regulation (EU) 2016/679 to a controller or (sub-) processor not subject to Regulation (EU) 2016/679, Article 28 SCCs apply only to controllers and processors that are subject to Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 (Article 2 of the Commission draft decision regarding Article 28 SCCs).

We note that under Clause 7(6) of the 28 SCCs, *"Where the data processor engages a sub-processor for carrying out specific processing activities (on behalf of the data controller), it shall do so by way of a contract which imposes on the sub-processor the same obligations as the ones imposed on the data processor under these Clauses"*. However, Clause 7(7)(b) further mentions that in case of international transfers, the parties may use the SCCs adopted on the basis of Article 46(2)(c) GDPR.

This raises the following comments:

- It is unclear to us why the Article 28 SCCs have been limited in scope to entities subject to the GDPR or Regulation 2018/1725, whereas they could be used between a controller based in the EU and subject to the GDPR and a processor established in a country providing an adequate level of protection on the basis of a decision of the Commission. For example, a sub-processor based in Argentina would not need to use the SCCs adopted on the basis of Article 46(7) GDPR, since such country already provides the adequate safeguard under Chapter V of the GDPR. We suggest to clarify that sub-processing agreement scan mirror the obligations of the Article 28 SCCs without requiring to incorporate the SCCs when the sub-processor is subject to the laws of a country for which the Commission issued an adequacy decision.
- Small variations appear between the Article 28 SCCs and the transfer SCCs, affecting the nature and the scope of some obligations for which the difference of drafting could create legal uncertainties. In the spirit of encouraging legal certainty and predictability, we suggest to align the two texts. Here are some examples of the differences between both texts that should be corrected:
    - While SCCs mention a deadline (48 h) for the processor to notify the controller of a data breach, the MODULE 2 of the SCCS do not mention such a deadline.
    - Whereas Article 28 SCCs refer to a priori *agreement* of the controller to hire a processor, the SCCs refer to a prior *authorization*.
    - Section 2, Clause 8 (Data Subject Rights) of the Article 28 SCCs mention a full list of data subject rights for which the processor shall assist the data controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights. Whereas such a list seems to mention the complete list of data subject rights under the GDPR (including portability, for example), the list in the SCCs is not that complete (and does not include data portability).

F. Transparency for the Data Subject

Publication of SCCs

The SCCs are a private contract to the benefit or a third party - the data subject. They thereby systematically generate and rely on private inter-party arrangements to protect the data subjects' fundamental rights under Article 8 CFR. In daily practice they are however mostly "secret law" that is dropped in a drawer of the controllers and processors and often withheld from the data subjects that should be the main beneficiaries of these arrangements.

For example, in the recent litigation with Facebook, the controller only sent us the raw text of the Commission decision (as available in EUR-Lex) but not a copy of the actual agreement signed by the parties. This behavior in plain sight of the SA and the Courts is rather extreme, but other controllers equally interpret their duty to only include the word "SCCs" in their privacy policy. Getting hold of the relevant documents regularly proves an exercise of months or even requires litigation for *noyb*. We therefore assume that ordinary data subjects do not receive the law that is meant to define their rights.

According to the transparency obligations under the SCCS, the data subject should receive a copy of the SCCs only upon request. Article 14(1)(f) GDPR requires the controller to communicate the reference to the appropriate suitable safeguards (in this case, to the SCCs) and the means to obtain a copy of them or where they have been made available. Nothin in the GDPR requires that this is solely done "on request". It seems very burdensome for data subjects, processors and controllers to require individual requests and answers to make these documents transparent.

Contrary to other contracts, the SCCs are not primarily a B2B arrangement, but a third-party beneficiary arrangement that is the basis to interfere with the rights of the data subject. Article 14(1)(f) GDPR also requires absolute access to these documents, which is why there is no basis for any form of confidentially of these documents that would limit the options to make them quickly available to the data subjects.

We would therefore urge the Commission to require a prior and systematic publication of the SCCs (e.g. a link in the relevant privacy policy or an internal page that is available to more limited circles of data subjects). This would be less burdensome for controllers – compared to countless individual requests – and would end the "hunt" for these crucial documents that are meant to provide fundamental rights to data subjects.

Transparency of Assessment of Third Country Law

Equally the various foreseen assessments of third country law are neither a matter of confidentiality nor business secrets, but highly relevant for the data subjects, as these assessments determine a third party interference with their rights. Any third country law or practice that interferes with the SCCs are an essential part of the "safeguards" (Article 14(1)(f) GDPR) and therefore falls under the GDPR's transparency obligations.

When any such assessment was brought to our attention, they were usually very superficial and controllers even mentioned that the assessment was done orally. We assume that the requirement to make such an assessment available to the data subjects will have positive effects with regards to the seriousness of these assessments.

We therefore suggest that these assessments should equally be made available.

Copy of the actual SCCs as signed and dated

In our understanding, the transparency obligation implies that controllers should not simply refer to a copy of generic text on the website of the importer, but to the actual copy of the SCCs as negotiated and signed by the parties involved (either electronically or on paper). We see too often SCCs referred to by the data exporter (controller) via a link on the website of the provider/importer, along with their general terms and conditions. In our opinion, the SCCs should be signed and mention the date of the signature of the SCCs. Such date and signature are important for the complete information of the data subjects and the supervisory authorities. Furthermore, the signature and the date are essential to assess the validity and the enforceability of the document, and in particular to enable the data subjects to invoke their third party beneficiary rights in front of a court.

For these reasons, we suggest to specify in the draft decision and in the SCCs that a copy of the actual SCCs (as signed and agreed) should be actively provided to the data subjects with the actual date of signature/formal agreement by both parties, even in cases where the Parties do not choose to use the optional Clause 6 ("Docking clause").

G. Other remarks

Obviously, an assessment of the proposed SCCs would not "undermine" the GDPR, and would require a full comparison of all elements of the SCCs with at least the core requirements of the GDPR. While neither the time of the consultation phase nor our resources allowed for such an extended review, we would nevertheless like to make the following observations on the current text:

Article/Clause number	Headline	Comment
Draft decision - Article 3	-	We welcome this effort towards information and transparency. However, the information by a Member State to the Commission in case of suspension of ban of a processing based on transfer should be further detailed and raises a few questions: - Does that imply that the Member States should communicate the entire decision to the Commission of the circumstances thereof? - Who should communicate the information/the decision to the Commission: the government of the Member State of the SAs directly to the Commission? - In some Member States, the decisions of the SAs are not always made public, and the names of the parties are sometimes redacted. Would this Clause. Considering the above, and in order to simply the chain of communication, we suggest to further specify that the full decision (unredacted, and including the names of the parties) should be communicated to the EDPB which will make it public on its website and communicate the decision to the Commission.
Draft decision - Article 6.2		For the sake of clarity, we suggest to clarify that Decision 2004/915/EU is also repealed.
Annex with standard contractual clauses	*Title*	We suggest to rename the "standard contractual clauses" to "standard data protection clauses on data transfers" (SDPC). This would align their name with Article 46(2)(d) GDPR and would make the content of these clauses clearer with an explicit reference to "data protection" and "transfer" in the title. It would also differentiate them from the previous clauses and the clauses adopted on the basis of Article 28(7) GDPR.
Section I - Clause 1 (b)	*Purpose and scope*	The reference to Annex I.A implies that, in case of a transfer from processor to processor, there will be at least three parties in addition to the processors (*i.e* at least one controller). However, the controller would not qualify as an "exporter" under the SCCs. We suggest to clarify in the relevant clause that the controller is a party to the SCCs but not an exporter.
Section I- Clause 2 (a)	*Third party beneficiaries*	It is not clear why the provisions listed in Clause 2 (a) are excluded from the third-party beneficiary clauses: even if most of these provisions cannot be enforced by the data subjects, they should still be in a position to invoke them as a violation of the SCCs to claim damages. Therefore, we suggest to clarify that the date subject can still invoke these provisions in relation to a claim for damages. However, the exclusion of the following clauses is acceptable since the data subject can neither invoke nor enforce them: - Clause 7 of Section II (*Liability)* under (*v*), - Clause 8 of Section II (*Indemnification*) under (*vi*) - Clauses 3(a), (b) (*Choice of forum and jurisdiction*)[8]
Section I – Clause 4	*Hierarchy*	This clause should allow for additional clauses if they increase the level of protection, instead of prohibiting all conflicting clauses as a general principle. Therefore, we suggest to mention that possibility.

[8] Without prejudice to our comment on Clause 3 below in this table.

Section II – MODULE ONE Clause 1.1	*Purpose*	The possibility given to use the data for another purpose that is not incompatible with the "specific purpose of the transfer" is problematic for the following reasons: - The reference in this Clause and in Annex I.B to the "purpose of the transfer" is not clear. The transfer is one of the processing operations as defined by Article 4(2) GDPR. The exporter processes the data for one or several purposes, that might be different from the ones of the importer. - Even if Article 6(4) GDPR allows for such further processing, we have strong reservations about the compatibility of this provision with Article 8 of the EU Charter of Fundamental Rights. However, should further processing without consent be made possible under this Clause, the lack of criteria as the ones defined under Article 6(4) GDPR will increase the risk of misinterpretation of what constitutes a "further processing compatible with Article 6 GDPR". Considering the above, we suggest - to modify this clause and Annex I.B with a reference to the description of the purposes of the processing pf the data by the exporter, and to delete the reference to the purpose of the processing; - to align this clause with the wording of Article 6(4) GDPR and explicitly include the criteria to determine whether a further processing will not be incompatible.
Section II – MODULE ONE Clause 1.2	*Transparency*	In order to strengthen the liability of the exporter towards the data subjects and enhance the enforceability of the SCCs, we suggest to mention that - the importer should inform the exporter of this further use before such use - the exporter can object to such use within a specific deadline - the exporter will be liable towards the data subjects not having objected in due time to the further processing.
Section II – MODULE I Clause 1.2 (c) MODULE II Clause 1.3 MODULE III Clause 1.3	*Transparency*	We suggest that the clause specifies that only Annex II of the SCCs may be redacted. In case of redaction, the data subject should be able to understand the concrete security measures in place. This would avoid a general description of these security measures in the SCCs, too often observed in practice. This means that the entire SCCs, including the Annexes (except Annex II in some cases) should be made available.
Section II – Clause 1.3 (a)	*Accuracy*	The text of this clause is not aligned with Article 5(1)(d) GDPR. We suggest to correct that.
Section II – Clause 1.5 (a)	*Security of processing*	The clause only refers to pseudonymisation and encryption of data whereas other measures are mentioned in Article 32(1) GDPR. We suggest to include them as well.
Section II – 1.5 (d) and (e)	*Security of processing*	We welcome the obligation imposed on the importer to notify any data breach to the exporter, and the cooperation with the exporter to inform the data subjects where necessary. We also suggest to define the term "where necessary" in this clause, since we do not see in which concrete cases such cooperation would (not) be deemed necessary.

Section II – 1.5 (e)	*Security of processing*	The clause provides that the data subjects should be notified of the data breach, unless disproportionate efforts are required. However, in such a case, the GDPR provides that a general communication to the public should take place. We suggest to include this option in the clause.
Section II – MODULE I Clause 1.6 MODULE II Clause 1.7 MODULE III Clause 1.7	*Special categories of personal data*	We welcome the fact that this clause addresses the protection of special categories of data. However, this definition of special categories of data is not in line with the definition under Article 9 since this clause also includes the data mentioned under Article 10 GDPR. The clause does not mention the general prohibition of processing of Articles 9 and 10 GDPR, and seems to further spepcify the obligations of the SCCs in terms of security. We suggest to align the definition and processing of special categories of data with the GDPR.
Section II – Clause 1.7	*Onwards transfers*	The last case (*iv*) refers to consent as a legal basis for onward transfer to a country without adequate protection. As the EDPB already recalled several times, this should only be possible in exceptional circumstances and should not be possible for massive transfers. We suggest to include this clarification.
Section II – MODULE II Clause 1	*Instructions*	See our general remark (under E) regarding the interaction between the present SCCs in MODULE II and the SCCs as proposed by the Commission on the basis of Article 28(7) GDPR. We suggest to streamline both approaches and texts.
Section II - MODULE II Clause 1.1 MODULE III Clause 1.2	*Purpose limitation*	The reference to "specific purpose of the transfer" in this Clause and in Annex I.B is not clear to us (see remark under MODULE ONE, Clause 1.1). A transfer is one processing operation as defined by Article 4(2) GDPR. The exporter processes the data for one or several purposes, that might be different from the ones of the importer. We suggest to modify this clause and Annex I.B with a reference to the description of the purposes of all processing operations by the exporter, and delete the reference to the purpose(s) of the transfer.
Section II – MODULE IV Clause 1.3	*Documentation and compliance*	This clause is too generic. We suggest to include further details, inspired by the pending clause in MODULES II and III. A reference to Article 24 GDPR or to a similar wording would be an option in this respect.
Section II – MODULE IV Clause 2 and Clause 3	*Local compliance with the clauses*	The clause restricts application of Clause 2 to cases where "the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU". We understand that the Commission wants to protect the data transferred outside of the EU only if they originate from the EU. However, we do not understand why such restriction is only applicable to Clauses 2 and 3 of the SCCs. We suggest to remove this restriction and make it applicable for all transfers to the controllers/importer under MODULE IV.
Section II – ALL MODULES Clause 2 (a)	*Local compliance with the clauses*	The sole reference to the laws of the third country is not sufficient to perform the assessment: as the Court of Justice stated in *Schrems II* (see § 94), the practices of the country should also be taken into account to perform an assessment of the safeguard put in place. We suggest to include a reference to practices of this country that are outside of any law, in addition (not as an alternative) to its laws.

Section II – ALL MODULES Clause 2 (b)	*Local compliance with the clauses*	- We note that the Court of Justice confirmed that the transfer should be suspended or stopped when the standard clauses are not or cannot be complied with, and therefore the protection of the personal data cannot be ensured (see § 106 of *Schrems II*). - The reference to the specific circumstances of the transfer and other elements is not clear to us: is the intention to perform a so-called "risk–based transfer analysis"? As developed in our general remarks (under D), we think that this approach is not supported by the GDPR and is even at odds with the Guidance provided by the EDPB on additional measures and the *Schrems II* judgement. Therefore, we suggest to further detail how to use these elements in the overall assessment and make it clear to controllers and processors that EU law requires a "law and practice" and not a "law or practice" approach. - The absence of requests from public authorities in the past should not be relevant in this case: as the Court of Justice of the EU developed in its judgement *Schrems II*, the level of protection should be guaranteed. If such law allows for access to data that goes beyond what is necessary in a democratic society, the conclusion should be that no appropriate safeguards for the data can be guaranteed in the third country, even without actual access to the data by the public authorities where the law provide for such an access.
Section II – ALL MODULES Clause 2 (d)	*Local compliance with the clauses*	It seems hard to understand how the assessment under (b) - which is is at the core of protecting the data subjects' rights - is made available to every relevant party, but not the concerned data subjects who's rights are on the line. We highly recommend to make this assessment available to the data subjects as well.
Section II – ALL MODULES Clause 2 (e)	*Local compliance with the clauses*	The sole reference to the laws of the third country, and not the practices, is not in line with the GDPR and the case-law of the Court of Justice. We therefore suggest to include a reference to such practices in the clause.
Section II – ALL MODULES Clause 2 (f)	*Local compliance with the clauses*	This clause refers to the possibility to consult the competent authority, "if appropriate". We suggest to further explain when such consultation is deemed to be appropriate. Furthermore, we are concerned about the role of the SA, which can be consulted by the exporter, or receive a communication by the exporter under the circumstances described under this paragraph (f). Once the SA has provided consultation at the request of the exporter, it will be difficult for the SA to act independently in case of enforcement or investigation that would occur after the contacts with the exporter. Moreover, the clause does not mention whether the SA should act after having being notified by the exporter of the additional measures adopted to continue the transfer. We therefore suggest to: - add a right of the data subject to be provided with this information to take necessary steps to enforce their rights and/or take practical consequences. - clarify in the draft decision that the consultation given by the SA is without prejudice of the SA to decide to open and investigation or to impose a coercive measure against the

		exporter and the importer; - clarify in the draft decision that the communication of the additional measure to the SA and the lack of reaction of the SA are without prejudice of the SA to decide to open and investigation or to impose a coercive measure against the exporter and the importer.
Section II – MODULES II and III Clause 4	*Use of sub-processors*	What seems more important in this context is to precise whether or not the processors already approved will actually be used by the importer, and not whether the importer *intends* to call upon their services. We suggest therefore to clarify in the clause that the exporter is always aware of the subprocessors actually and not potentially hired by the importer of data.
Section II – MODULE I Clause 5	*Data subjects rights*	Some data subject rights, such as data portability or the right to be forgotten, are not mentioned in the list of rights. Considering that the level of protection cannot be undermined at the occasion of a transfer (see our general remark under A above), all the data subject rights (and in particular the news rights granted by the GDPR in comparison with the Directive) should be mentioned in this clause. We refer to our general remark under A.
Section II – MODULE I Clause 5 (d)	*Data subjects rights*	The wording of the clause on automated-decision making is not aligned with Article 22(1) GDPR. We therefore suggest, among others, to delete the reference to "without human involvement", and use the wording of Article 22(1) GDPR to avoid any confusion.
Section II – MODULE I Clause 5 (f)	*Data subjects rights*	The clause refers to the right of the data subject to submit a judicial review, whereas the correct term should be judicial redress or remedy (see Article 79 GDPR). We suggest to correct that wording accordingly.
Section II – MODULE 2 Clause 5 (b)	*Data subjects rights*	The cooperation between the importer and the exporter should take place "taking into account the nature of the processing". We suggest that the Commission further explain the clause accordingly.
Section II – MODULES 1, 2 and 3 Clause 6 (b)	*Redress*	The wording "the importer accepts the decision of the data subject" does not create any obligation for the importer to comply with the decisions of the SA or the competent courts. Therefore, we suggest to change the wording as follows: "the importer accepts the jurisdiction of the competent authority where the data subject will decide to file a complaint, and the jurisdiction of the competent court where the data subject filed a dispute".
Section II – MODULES 1, 2 and 3 Clause 6 (b) and (c)	*Redress*	Considering that we already observed that some importers mention in their contractual terms that all claims against them by data subjects could only be individual claims (excluding class actions, collective redress and similar claims, but also claims based on collective interests), we suggest to mention in the clause that all administrative or judicial proceedings available to the data subjects shall be accepted by the importer, and to mention an explicit prohibition to limit contractually the redress available to the data subjects. Considering that some Member States will soon open the possibly to file representative actions under article 80.2 GDPR, we also suggest to add this provision under litera *(c)*.

Section II – MODULES 1, 2 and 3 Clause 6 (b) and (c)	*Redress*	We do not see the reason why no redress under Clause 6 is granted to the data subject whose data were transferred to a controller outside of the EU. We suggest to make this clause applicable to all modules.
Section II – ALL MODULES Clause 7	*Liability*	- The rationale behind the difference of drafting between litera *(c)*, applicable to MODULES 1 and 4 and litera *(c)* and *(d)*, applicable to MODULES 2 and 3 is not clear.[9] We suggest to merge both texts to simplify the wording. - The exclusion of most of the clauses from the third party beneficiary rights is not justified. See our comment under Clause 2 in this regard, where we suggest to broaden the clauses on which the third parties could rely. - The text of litera *(e)* applicable to MODULES 1 and 4 and the text of litera *(f)* applicable to MODULES 2 and 3 should include *"any other third party"* next to *"sub-processor"*. We do not see why the importer could escape its liability by invoking the conduct of another party that is not a sub-processor (but yet a provider under its responsibility).
Section II- Clause 9	*Supervision*	The clauses contain multiple references to the competent authorities in various different instances: - Article 3 refers to the competent authorities exercising their corrective powers and notify a ban or suspension of a transfer to the Member State - MODULE 1 - Clause 1.5 (d) refers to *"the competent authority within the meaning of Clause 9 of Section II"* and 1.9 (b) for the notification of a data breach by the exporter - MODULE 2 and 3 - Clause 1.6 (d) and Clause 1.9 (e) requires the notification of the competent SA by the data importer - MODULE 4 - Clause 1.1 (c) refers to the cooperation with the competent authorities - Clause 2.2 (d) and 2.2 (f) refers to the competent authority to which the parties have to make their assessment available - Clause 3.1 (d) (the importer shall make the documentation available to the competent authority in case of access by public authorities) and 3.2 (b) (the importer shall make the documentation available to the competent authority regarding challenges of requests of access by public authorities) - MODULE 1 - Clause 6 (b) (i) and (g): complaint with the competent supervisory authority It seems therefore that only the SA designated under this Clause would act as the competent authority. This can raise some issues, for example, as to the competent authority where the

[9] The only difference is the last line of litera *(d)* in the text applicable to MODULE 2 and 3 is the following text: *"where the data exporter is a processor acting on behalf of a controller, the controller under the GDPR"*.

		data subject could file a complaint, since the competent authority designated in Clause 9 may be a different authority than the one of the Member State where they live or work (see Article 77 GDPR). That would imply that the data subjects may file a complaint against the exporter to any relevant SA, while they would have to file the same complaint against the importer to a different SA according to Clauses 6 (b) and 9. This would be too complex for the data subjects and would even create confusion within the SAs themselves. Clause 1.5 (d) refers to *"the competent authority within the meaning of Clause 9 of Section II"* and 1.9 (b) for the notification of a data breach by the exporter. The competent authority is defined under Clause 9 as *"the one with responsibility for ensuring compliance by the data exporter with the GDPR as regards the data transfer"* and invites the parties to designate this authority in the Clause. - Doing so, the Clause ignores that fact that all SAs have a general competence according to Article 55 GDPR (and possibly Article 66). If the intention of the Clause is to refer to the lead SAs, by reference to Article 56 GDPR, we suggest that the text makes it clear, to avoid any confusion. - Even in this case, the Clause seems to ignore that the exporter might not be subject to the supervision of only one authority in the EU. This may be the case where the data exporter does not have a main establishment in the EU[10] or is subject to the GDPR by virtue of Article 3(2) GDPR. However, only this last case is addressed in the alternative text suggested in Clause 9.1. - In the alternative clause, the competent authority will be the one *"of the Member State where the data subjects whose personal data are transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located"*. This Clause does not address the case where data subjects are located in several member states. In such a case, several SAs would be competent, and not only one. - Considering the difficulties to interpret the Clause, the freedom left to the Parties to designate the competent authority open the door for forum shopping, which is explicitly rejected by the EDPB. In these circumstances, we would suggest to use the criteria of the GDPR to designate the competent authority and to make reference to these criteria in the Clause. - The application of Clause 9.2 may raise the same problem since the data importer submit itself to the competence of one SA, whereas data subjects may file a complaint to different authorities, all being competent to investigate the case. On the basis of the above, we suggest to redraft the Clause to be consistent with the GDPR, the rights of the data subjects and the respective competences of the SAs.

[10] See Guidelines for identifying a controller or processor's lead supervisory authority, WP 244, Section 2.2.

Section III – Clause 1 (d)	*Non-compliance with the Clauses and termination*	The rationale behind the difference of choice given to the exporter between MODULES A, 2 and 3 and MODULE 4 is not clear: why could the controller/importer be obliged to destroy the data whereas the option is given the data exporter in MODULES 1,2 and 3? We suggest to clarify this point. On a general note, we think that the automatic destruction of the data might impair the investigations by the SA: as from the moment the data are deleted and were not copied by the importer, the evidence of the violation might prove to be impossible. We therefore suggest to insert a wording allowing for data that might serve as evidence to establish the violation of the SCCs to be copied and stored with restricted access by the data exporter at the disposal of the SA.
Section III – Clause 3	*Choice of forum and jurisdiction*	In so far (a) and (b) refer to the choice of jurisdiction of the parties for any dispute arising from the SCCs, it is understandable that these two provisions are excluded by the list mentioned in Clause 2 (a) (see our comment above). However, Clause 3 (c) further states "*legal proceedings by a data subject against the data exporter and/or data importer may also be brought before the court of the Members State where the data subject has his/her habitual residence"*. - The term "also" seems to imply that the choice of jurisdiction made under (a) and (b) is binding on the data subject, whereas this provision only concerns the relationship between the data exporter and the data exporter, and is furthermore explicitly excluded from the list contained in Clause 2 (third party beneficiary). - Moreover, Article 77 GDPR opens the possibility to file a complaint against the controller of the processor with any SA, mentioning as an example the SA of the Member State of their habitual residence, place of work, or of the alleged infringement, whereas this Clause seems to restrict this possibility. - Furthermore, Article 79 GDPR opens the right to bring a proceeding against a controller or a processor before the courts where the controller or processor has an establishment, or where the data subjects have their habitual residence, whereas this Clause seems to restrict this possibility. On the basis of the above, we suggest - to clarify the exclusion of the third party beneficiary right under Clause 2 of Section 1 and Clause 1 of Section 3; - to specify that the choice of jurisdiction under Clause 1 of Section is without prejudice for the rights of the data subject to lodge a complaint before the SA as per Article 77 GDPR and to file a judicial proceeding before in accordance with Article 79 GDPR.