VISCHER

FREQUENTLY ASKED QUESTIONS (FAQ)

NEW EU STANDARD CONTRACTUAL CLAUSES FOR DATA TRANSFERS TO NON-WHITELISTED THIRD COUNTRIES

taking into account the version 2.0 of the EDPB's recommendation 01/2020

By David Rosenthal, VISCHER AG[1] (translated from German[2])

The following questions relate to the standard contractual clauses for data transfers to third countries (**SCCs**) adopted by the European Commission on June 4, 2021, i.e. within the meaning of Art. 46 EU General Data Protection Regulation (**GDPR**). For the standard contractual clauses for processors (**SCCs-DPA**) see question 44. The commentary is based on the English version of the SCCs. Practical advice on the implementation of the new SCCs can be found in question 45. More information on the creation of an Intra-Group Data Transfer Agreement (**IGDTA**) (including an extensive checklist) is in question 46 and Transfer Impact Assessments (**TIA**) are addressed in question 41.

The Federal Data Protection and Information Commissioner (**FDPIC**) has not yet commented on the validity and recognition of the SCCs under the Swiss Data Protection Act (**CH DPA**). This FAQ will be updated as soon as this happens.[3]

Version	Most important changes
June 22, 2021	First draft (English version only as a machine translation)
July 13, 2021	Manual translation, newly introduced question 7 (transfers to non-whitelisted third countries, if the importer is subject to the GDPR); clarifications on the meaning of "nature of processing" (question 18); the new question 20 (EU Member States), 33 (sub-processor in Europe) and 46 (IGDTA); more details on questions 40 and 41 (Schrems II and TIA) and the list of flaws in the SCC (42).

Questions and feedback: dataprivacy@vischer.com

---

1 Contributors: Samira Studer, Mladen Stojiljkovic, Elias Elmiger (all VISCHER). Many thanks to Phil Lee (FieldFisher), Christian Schröder (Orrick), John Magee (DLA Piper), David Vasella (WalderWyss) and various others for their expert input to this FAQ. The author can be reached at drosenthal@vischer.com.

2 With the great support of Mairi Weder-Gillies (VISCHER); the original German master version is unofficially available here: https://www.rosenthal.ch/downloads/VISCHER-faq-scc.pdf.

3 Unofficial permalink: https://www.rosenthal.ch/downloads/VISCHER-faq-scc-en.pdf.

1. What are the most important changes?

The most important changes versus the old standard contractual clauses are:

- More constellations of data transfers to non-whitelisted third countries are now covered by a single, modular document than before (question 11). Even a processor in the European Economic Area (**EEA**) who has a client in a non-whitelisted third country will be able and obliged to use the SCCs in future (question 30). The new SCCs also regulate more than before in terms of content. There is no longer any need for a separate data processing contract, as the new SCCs contain all the necessary provisions (question 41).
- There is unlimited liability for data protection breaches, both among the parties and towards data subjects (question 38). The SCCs may not be changed or restricted. Nevertheless, there is already discussion about whether and to what extent this liability can be limited after all, at least between the contracting parties. The question will be particularly important for service providers (their workaround: they will conclude their contracts with European clients only through their European companies - so the new SCCs will no longer be used on the client side).

- The SCCs provide for additional preventive and reactive provisions to protect data from foreign access by authorities (question 40). The parties must warrant that they have "no reason to believe" that in the destination country such accesses exist without any guarantee of legal recourse, and if an authority does attempt to access the data, they must inform the data subject and try to prevent the access. For this purpose, a *Transfer Impact Assessment* (TIA) must be carried out. In this way, the European Commission (rightly) advocates a risk-based approach, which is now also accepted[4] (with some reservation) by the European Data Protection Board (**EDPB**).
- The information and notification obligations are increasing. Now even sub-processors must inform the data subjects about a contact option (question 35) and about access attempts by foreign authorities (question 40). Data subjects may also request to see the SCCs concluded by the parties. All obligations for the benefit of data subjects can now be directly enforced - or enforced by organisations such as the *European Center for Digital Rights* (**NOYB**) [5] (question 36).

2. What risks does conclusion of the SCCs entail for the exporter and importer?

The conclusion of the new SCCs entails, among others, the following new or increased risks:

- Unlimited contractual liability for data protection breaches, both towards the other parties in the SCCs and towards the data subjects. These can also be enforced before a variety of foreign courts.
- Because the SCCs may not be changed and cover more topics than before, their introduction in existing contractual relationships can upset the existing balance - for example with regard to cost bearing, risk distribution and liability.
- Data subjects or organisations such as NOYB can take legal action to enforce compliance with the SCCs. They can also inspect the completed SCCs, even if certain parts are redacted. Since there are more obligations than before, more can be claimed.
- The exporter is ultimately also responsible for the importer's compliance with the SCCs.

---

4 https://edpb.europa.eu/news/news/2021/edpb-adopts-final-version-recommendations-supplementary-measures-letter-eu_en.

5 https://noyb.eu/.

- The effort required for correct implementation will increase significantly. For example, the parties must document all activities and submit this documentation to the supervisory authority upon request. They must also inform each other of incorrect or incomplete data. If the UK does not accept the EU's new SCCs (at the moment the indications are not promising), everything will become even more complicated because two different treaties will then be required in dealings with non-whitelisted third countries. Switzerland, on the other hand, is likely to recognise the new SCCs.
- Service providers in Europe will also have to impose a reduced version of the SCCs on their clients in non-whitelisted third countries once they start to process personal data for them. Their liability risk increases - as does that of their clients.

3. When do we have to start using the new SCCs?

For this purpose, a distinction must be made as to whether a data transfer is taking place under the GDPR or under the CH DPA.

Under the GDPR, the new SCCs must be used in [all] new contracts from September 28, 2021. (Old) SCCs signed by September 27, 2021 must be replaced by December 27, 2022. So anyone who still absolutely wants to use the old SCCs must have done so before September 28, 2021.

The long deadline of December 27, 2022 is deceptive as the use of the old SCCs is only permissible after September 28, 2021 if and to the extent that the data processing in question does not change and continues to be adequately protected[6]. In practice, these conditions will probably not be met in many cases, at least not according to the traditionally strict interpretation of some EU data protection authorities. It will almost never be the case with an Intra-Group Data Transfer Agreement (**IGDTA**), under which, by its very nature, a large number of data transfers are processed and, based on general life experience; the data processing will also change by December 27, 2022, as will the parties (e.g. acquisition of a new company). Additionally, the EU data protection authorities will probably take the view that without additional clauses (such as a "defend-your-data" clause, question 40), the existing SCCs offer insufficient protection. Therefore, IGDTAs in particular should be transitioned to the new SCCs by September 27, 2021.

Under the CH DPA, the situation is more relaxed. The deadlines set by the European Commission are not binding in Switzerland. As long as

---

6 Article 4 of Decision C(2021) 3972 of 4 June 2021: "[...] provided the processing operations that are the subject matter of the contract remain unchanged and that reliance on those clauses ensures that the transfer of personal data is subject to appropriate safeguards".

the old SCCs can be considered materially sufficient, which we currently still believe to be the case, they can be used for as long as desired. This also applies under the revised CH DPA, as it does not increase the requirements for cross-border disclosure of personal data. What changes is the mechanism of the obligation to submit data to the FDPIC (question 25). For various reasons the FDPIC can be expected to demand the use of the new SCCs and declare the old SCCs to be inadequate in his opinion. This point of view is not binding, but it will have an impact: In combination with the fact that only the new SCCs may be used in the EU, they will ultimately become generally accepted in Switzerland. A special Swiss approach is unrealistic; even the FDPIC's own SCCs have never really gained widespread acceptance. It is easier to use the same template as the rest of Europe. It can therefore be assumed that the view will prevail that the new SCCs are also required under the CH DPA, even if there is no legal basis for this, since neither the legal nor the factual situation has changed and there is thus no (legal) reason why the previous SCCs should suddenly no longer suffice. If this is the case, however, many companies will see themselves endeavouring to adopt the new SCCs for the purposes of the CH DPA until the revised CH DPA comes into force. The driving force here will be that under the revised CH DPA, (possibly) intentional cross-border disclosure of personal data without adequate protective measures will be a criminal offence. Hardly anyone will want to take this risk. Until then, however, Swiss data processors will be in little danger if they still use the old SCCs - even if the conditions of the European Commission are not met.

Companies that must comply with both the GDPR and the CH DPA should, in view of this starting position, align themselves with the requirements of the GDPR. This can also affect companies that are "only" subject to the GDPR on the basis of Art. 3(2) GDPR and only process data in Switzerland: If a processing of personal data is subject to the GDPR, the requirements of the GDPR must also be observed when transferring data from Switzerland to a third country (here, the GDPR differs from the Swiss regulation, which is linked to the disclosure from Switzerland).

4. When can we start using the new SCCs?

The new SCCs may be used for the purposes of Art. 46 GDPR since June 27, 2021.

In Switzerland, they can be used immediately. However, it is advisable to wait until the FDPIC has recognised them (question 9) because if it does not recognise them, the owner of a data file is obliged to submit it to the FDPIC for review (Art. 6(3) CH DPA). The "simplified" notification by means of a simple letter (Art. 6(3) Ordinance to the Federal Act on Data Protection Act, **CH DPO**) only applies to SCCs recognised by the FDPIC.

5. Where can I download the new SCCs?

At https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj they can be downloaded in all EU languages, in both HTML and PDF formats. It is also possible to compare languages. Several private providers now also offer preconfigured versions and "generators" (see para 12).

6. In which cases do we have to use the new SCCs?

There is no legal obligation to use the new SCCs.

However, under the GDPR, the new SCCs will, in some scenarios, be the only reasonable method to legally and adequately secure the disclosure of personal data to a non-whitelisted third country. Other methods such as "Binding Corporate Rules" (**BCR**), consent or the other exceptions will not be effective in some cases. It is possible that in time the European Commission will publish another set of SCCs for the disclosure of personal data to non-whitelisted third countries but this will happen at best at a much later point in time, if the existing SCCs prove to be unsuitable or too impractical (cf. the shortcomings in question 42).

It is conceivable under the GDPR that individual supervisory authorities will publish further SCCs, which must be approved by the European Commission (Art. 46(2)(c) GDPR), but this is not expected at the current point in time (except with regard to one limitation existing with regard to one deficiency of the new SCC, see question 7).

Finally, the GDPR provides for the use of individual contracts for data transfers to non-whitelisted third countries but these must be approved by the respective competent EU supervisory authority (Art. 46(3)(a) GDPR). In our opinion, this case is conceivable, for example if the SCCs have to be used in a modified form in order to correct errors that they contain (question 22) or because the use of the SCCs as intended would be unlawful, as long as the adaptation does not affect the protection of the data subjects.

Under the CH DPA, the situation is less strict and it is quite conceivable that alternative contract templates could be used instead of the SCCs - possibly with the consequence that these must be submitted to the FDPIC. Unlike under the GDPR, under the current and revised CH DPA the data exporter remains responsible for ensuring that the contracts it uses provide appropriate protection. Nevertheless, under the revised CH DPA, the FDPIC will be able to take supervisory action against what it considers to be inadequate contracts. It is conceivable that the FDPIC will accept alternatives to the SCCs if the EU SCCs prove to be deficient or unsuitable in certain respects. It is also conceivable that the FDPIC will accept the SCCs being developed by the UK.

7. Can the new SCCs be used for transfers to non-whitelisted third countries even if the importer is subject to the GDPR?

Yes, but in this respect the European Commission has made a mistake, which is likely to be corrected soon in one form or another, as the new SCCs have *not* been approved for this case. However, sanctions are not to be expected here for the time being.

Recital 7 of the Implementing Decision C(2021) 3972 of 4 June 2021 specifies in which cases SCCs "may" be used. This is not to be taken at face value because the GDPR only regulates where the SCCs may be used to fulfil a requirement of the GDPR, but not where contractual clauses adopted by the European Commission may and may not be used.

Recital 7 describes both the authorised exporter and the authorised importer:

- Exporter: If the exporter is located in the EEA, no further questions arise. This also applies if the exporter is not located in the EEA but is subject to the GDPR by virtue of Art. 3(2) GDPR. For exports to non-white-listed third countries, the exporter has already had to comply with the provisions of Art. 44 et seq. The SCCs can and should be used for these purposes. This is also reflected accordingly in Clause 13 of the SCCs (where a distinction is made between the controller or processor who has a representative pursuant to Article 27 of the GDPR and the controller or processor who has not appointed one).
- Importer: Uncertainties have arisen because recital 7 states that SCCs "may" be used only in cases where the processing of the data by the importer is not covered by the GDPR. This is wrong and in our opinion irrelevant. According to Art. 44 et seq GDPR, it does *not* matter whether the importer falls under the GDPR, but whether it is located in a whitelisted or a non-whitelisted *third country.* Even if the recipient in the non-whitelisted third country falls under the GDPR (e.g. a US online service that tracks users in the EEA), the EEA company sending it data will agree with it on SCCs. This has always been the case and there are no apparent indications of a change in the system. Conversely, the conclusion of the SCCs is not necessary if the recipient is located in a *white-listed* third country - regardless of whether the recipient falls under the GDPR or not. However, it may do so anyway, because the GDPR does not have a *numerus clausus for* data protection contracts and does not prohibit their conclusion even where such contracts are unnecessary - as long as such contracts do not prevent the parties from implementing the GDPR where it applies. Excessive use of SCCs must therefore be permitted, contrary to Recital 7. It must even be permissible to conclude the SCCs between two entities within the EEA if this makes sense in a

specific individual case (e.g. as a data processing agreement in multilateral contracts where some of the parties are in third countries and others are not). The fact that the "importer" in the definition in Clause 1(b)(ii) is referred to as an entity "in a third country" does not change this.

In addition, where SCCs are concluded with processors outside the EEA, it is extremely difficult in practice to determine with legal certainty whether the processor as such is actually subject to the GDPR or not. Normally, the processor will not be subject to the GDPR if it does not itself "track" natural persons in the EEA or engage in "targeting" for (its) products or services. However, the EDPB is stricter in its Guidelines 3/2018 (p. 20 et seq.) and considers processors established in a third country to be subject to the GDPR if they are involved in the targeting or tracking of their controller. This is debatable, but it does not change anything here, because Recital 7 cannot apply in this way and is also not reflected in the SCCs. If Recital 7 were to be implemented literally, the SCCs would not be allowed to be concluded in these cases, but without the SCCs, the transfer of data would not be permitted in these cases, unless one of the other instruments under Article 46(2) of the GDPR or one of the exceptions under Article 49 of the GDPR would apply by way of exception. The use of such processors in non-whitelisted third countries would be de facto prohibited as of 28 September 2021. This was certainly not the intention of the European Commission. It simply made a mistake (with recital 7, the European Commission possibly tried to give an answer to the joint opinion of the EDPB and the European Data Protection Supervisor on the draft of the new SCCs).

There is, however, a deeper reason for the Commission's comments, which suggests that this is not just an oversight. It is about the fundamental question of when Chapter V of the GDPR (which regulates international transfers) applies at all. There are opinions according to which it does not apply if the importer itself is subject to the GDPR. This does not really make sense. If this opinion were correct, "Schrems II" would never have happened, because the transfer of user data to Facebook in the US would have been legal in the first place even without *Privacy Shield* or the old SCC: The transfers would simply have not triggered the restrictions of Chapter V, if one assumes that Facebook US is indeed subject to the GDPR due to Article 3(2) of the GDPR. However, this opinion ignores the fact that compliance with the GDPR in the US - especially in the case of lawful access by public authorities - cannot really be enforced for data located in the US.

In the joint opinion of the EDPB and the European Data Protection Supervisor on the draft of the new SCC[7], the two bodies had already asked the Commission to only comment on the cases for which the new SCC were approved, but not on what is considered a transfer that is subject to Chapter V of the GDPR. The EDPB is currently preparing its own opinion on this point and should it (as is expected) conclude that transfers to non-whitelisted third countries are subject to Chapter V of the GDPR even if the importers are subject to the GDPR, then it will presumably ask the Commission either to extend the authorisation of the new SCC to cover this scenario or to issue new SCC for it.

Until then, the problem is that Art. 1(1) of the act implementing the Commission's approval of the new SCCs[8] states that the new SCCs only provide adequate protection where the importer is not covered by the GDPR. In practice, pending the clarification of the situation, there are two options:

- For the scenarios not formally covered, the existing SCCs are continue to be used, as in the case of transfers from the UK. If the contracts are concluded by September 27, 2021, they can in principle be used until December 27, 2022 (see, however, question 3), by which time the above situation should have been clarified.
- The new SCCs are used as if they were approved for the scenario discussed here. Their use is certainly not prohibited. The only question is whether the new SCCs are considered approved for the scenario discussed here and whether the exporter can therefore rely on Art. 46 GDPR for such transfers. This can be justified as follows: It is undisputed that the new SCCs are approved. Art. 46 GDPR only requires that SCCs are used which, firstly, are approved and, secondly, constitute "appropriate" safeguards. The new SCCs fulfil this requirement, because if they are considered "appropriate" for an importer who is not subject to any legal regulations, they must *a maiore ad minus* provide suitable protection for an importer who must also comply with the GDPR and otherwise fulfils all the requirements of an importer under the new SCCs. In our opinion, this makes up for the fact that the new SCCs are formally approved only for more problematic transfer scenarios and is in any case not in conflict with the wording of Art. 46(2)(c) GDPR.

---

7 In it they wrote (portions highlighted by us): "In view of the above and of the title [of] the Draft Decision, the EDPB and the EDPS understand that the Draft Decision **does not cover**: Transfers to a data importer not in the EEA but subject to the GDPR for a given processing under Article 3(2) GDPR [...]. Keeping this in mind, for the avoidance of doubt, the EDPB and the EDPS **recommend** the Commission to clarify that these provisions are only intended to **address the issue of the scope of the** Draft Decision and the draft SCCs themselves, and **not the scope of the notion of transfers**." (https://bit.ly/3gSC27q).

8 Dated June 4, 2021, C(2021) 3972.

We generally recommend the latter approach insofar waiting is not a reasonable option. We assume that the data protection authorities will not take action against companies that proceed in this way. A representative of the Bavarian data protection authority in Germany has already made comments to this end.

8. Are there cases where we are not allowed to use the new SCCs?

No, from a purely legal point of view, SCCs may be used in any scenarios. But: as "authorised" SCCs in the sense of the GDPR, they are only valid in the cases provided for by the SCCs themselves. There is thus both an official and an unofficial area of use of the SCCs. An *official* use takes place as a safeguard in the sense of Art. 46 GDPR between an exporter who falls under the GDPR and an importer who is located in a non-whitelisted third country. An *unofficial* use would be, for example, if the importer, in addition to its headquarters in an non-whitelisted third country (e.g. USA), also maintains a branch office in a white-listed third country (e.g. Switzerland) or in the EEA, which is of course also bound by the contract, even if data transfers to the branch office do not require SCCs.

On the question of using the new SCC in the event that the importer is located in an unsafe third country but is itself subject to the GDPR, see question 7.

Another question is whether SCCs also qualify as authorised SCCs for the purposes of Art. 28(7) GDPR if they are used as a data protection agreement between two parties in the EEA or a whitelisted third country (see question 44). This scenario may occur in an IGDTA (question 16).

9. Are the new SCCs recognised by the FDPIC? Do they even need his recognition?

No, so far they have not (yet) been recognised. Recognition is not legally required - it is the responsibility of the exporter of personal data to ensure adequate protection.

However, Art. 6(3) CH DPA provides that contractual safeguards (which is basically what SCCs are) must be submitted to the FDPIC for his opinion. If such safeguards are recognised by the FDPIC (as the the existing SCCs have been), a simple letter to the FDPIC stating that the company in question is going to apply them is sufficient (Art. 6(3) CH DPA).

It can therefore be assumed that the FDPIC will recognise the SCCs in one form or another. If he did not, he would be inundated with requests for his review, which would be practically unmanageable. The question that arises is whether he will recognise them in their "pure" form (as adopted by the European Commission) or whether he will allow or require modifications to adapt them to Swiss conditions (we

believe this is not necessary: question 24). Until this is done, we recommend holding off on their use.

From a Swiss perspective, the SCCs also mean that importers are subject to stricter rules than would apply to them under the CH DPA. This is because the SCCs provide for very far-reaching obligations that sometimes even exceed the level of the GDPR.

Under the revised CH DPA, recognition by the FDPIC will mean that the FDPIC no longer has to be notified (Art. 16(2)(d) revised CH DPA). On the other hand, anyone who uses a contract template that is not or no longer recognised will still have to report it to the FDPIC (Art. 16(2)(b) revised CH DPA). We expect that the FDPIC will revoke the recognition of the old SCCs after a certain period of time, which means that they can continue to be used, but new contracts or contract amendments will have to be reported to the FDPIC and it will probably also have to be explained to the FDPIC why they are still considered sufficient to ensure "appropriate data protection" (which is required by Art. 16(2) revised CH DPA).

10. Do the SCCs have any retroactive effect?

Formally, the SCCs have no retroactive effect. However, there are two things to note:

- First, the new SCCs provide that the parties must warrant that they have no reason to believe at the time of agreeing the SCCs that they cannot comply with them due to the importer's domestic law (Clause 14(a), introduction of Clause 8). In contrast to the previous SCCs, no further warranties are required. This means that the SCCs per se can only be concluded without breaching them once the previous legal situation in relation to this has been clarified. In practice, however, this is unlikely to happen very often. On warranties, see question 39.
- Second, the new SCCs provide for a number of obligations, primarily on the part of the importer, that apply immediately, including certain information obligations (question 35). This also means that in practice the importer's existing measures usually have to be adapted before the new SCCs can be concluded.

11. Is there a "de minimis" rule, i.e. cases where the SCCs cannot be agreed?

No. However, this is not an SCC issue, but rather a question of the applicable provisions of the GDPR or the CH DPA on the transfer of personal data to non-whitelisted third countries. The requirements stipulated apply to all transfers of personal data to non-whitelisted third countries, even if they are only of a minor nature or do not appear to be particularly sensitive. The fact that this is often not

complied with in practice (e.g. in the context of the transfer of a single e-mail to a recipient in the USA) is another matter.

12. How do we handle the new SCCs in practice? How do we "choose" the Modules?

The new SCCs cannot be validly adopted in their entirety in their current form. They contain contractual clauses for four different case scenarios that are used alternatively or in parallel. This means that it must first be decided which scenario(s) are at issue and the corresponding elements of the EU SCC must be selected accordingly. Based on this, the terms of the contract can be agreed based on the wording of the EU SCC.

The colleagues from WalderWyss have published an illustrative presentation of the individual case constellations and which modules of the SCC are to be used (see figure).[9]

There are basically three ways in which the new SCCs can be used, i.e. agreed upon, against this background:

- The provisions to be applied are selected from the EU SCC text and combined in a new document. There are already various law firms that offer such pre-customized templates or have designed "generators" for their creation.[10] When using these offers, however, it is important to pay close attention to whether adjustments still need to be made; in addition to selecting from the four Modules, there are various other options that need to be configured. It is also not possible to only focus on the module designations highlighted in grey (references to the Modules are sometimes also found in the text, e.g. in Clause 14(e) and (f); Clause 7, on the other hand, is optional for all Modules).

  A further limitation of this approach is that the clause of the SCCs governing the onward transfers of data by the importer refers to the complete clauses (i.e. the SCCs with *all* Modules), which are missing in this approach. There is a residual risk that the omission of Modules means that the importer cannot rely on the

---

9 https://datenrecht.ch/neue-standardklauseln-uebersicht-wann-sind-welche-module-zu-verwenden/.

10 Public: https://www.essentialguarantees.com/scc/, https://www.taylorwessing.com/de/online-services/scc-generator (TaylorWessing), https://bit.ly/3qeBI7b (WalderWyss); an SCC generator has also been announced by Bird & Bird, Orrick and LauxLawyers. The links will be provided here as soon as they are available to us.

omitted Modules (as they are no longer part of the "clauses") and thus has fewer options for onward transfers. However, we consider the risk to be relatively low; this editorial error of the SCCs has also gone largely unnoticed so far.

- A contract is concluded (e.g. in the form of a cover sheet) to which the complete SCCs are attached and in which it is determined which Module(s) of the SCCs are to apply in which scenario. The cover sheet can also determine which options are selected and how the individual fields and attachments are to be completed. This variant has the disadvantage that it leads to a longer contract, but at the same time there is no need to check whether the parts from the SCCs template have been compiled correctly. The text adopted by the European Commission can be adopted in its entirety.
- The same approach is used as in the foregoing bullet, but instead of attaching the SCCs as an annex, they are "only" included by reference, together with the selection of the relevant Modules and options - just as GTCs can also validly become part of a contract if they are correctly referenced and made available to the parties.[11] The permissibility of this approach is not determined by the GDPR, but by the applicable contract law. Under Swiss law, this approach is permissible: The content of the contract is clearly determinable for the parties and it is accessible at any time via the internet, given that it is an official decision by the Commission. However, a clear reference to the official version of the SCCs template is important, if possible with a corresponding internet link to the official website of the EU. The validity of this approach is apparently also accepted under German law. This "incorporation by reference" is the most streamlined approach.

In our view, all three variants are legally equivalent. In practice, we expect that in standard situations (e.g. contract with a cloud provider) the first variant will prevail. In an IGDTA or where several Modules apply in parallel, the second or third variant will be preferred.

13. Do the new SCCs have to be signed by hand or is an electronic signature sufficient?

No, contracts based on the new SCCs do not have to be signed by hand. Annex I.A of the Appendix refers to the "signature" of each individual party; Clause 7 also refers to a party "signing" the SCCs.

In our opinion, however, all that is required is - as before - proof by text, i.e. the content of the declaration of intent of the party binding

---

[11] Gauch/Schluep/Schmid, Schweizerisches Obligationenrecht Allgemeiner Teil ohne ausservertragliches Haftpflichtrecht, 2008, N 1140b.

itself to the SCCs must be recognisable and recorded in text form. This requirement can be fulfilled by "click" declarations. Contracts confirmed by means of simple signature systems such as "DocuSign" or "Adobe Sign" also fall into this category. If this were not the case, the conclusion of SCCs in the online context would simply no longer be possible. There is no reason to assume that this was the intention.

14. What should be considered when adjusting existing contracts with the previous SCCs?

The following points should be noted in particular:

- The Appendix of the new SCCs requires more information than was required for the previous SCCs (question 18).
- The technical and organisational measures (**TOMS**) must cover additional aspects under the new SCCs and be more detailed (question 17).
- The new SCCs regulate more than the previous SCCs (e.g. liability), and also require that these additional regulations take precedence. This can lead to parts of the previous contract (e.g. a data processing agreement) suddenly being in conflict with the new SCCs and to a change in the distribution of risk between the parties.
- Because the new SCCs can be used in more case scenarios, it may be necessary to cover these as well (question 15).
- The new SCCs are currently only approved for transfers of data under the GDPR. Whether they can also be used to safeguard data transfers under other data protection laws must be examined separately. For the UK, for example, this is not yet the case (question 21). The FDPIC has also not yet recognised the new SCCs for exports from Switzerland (question 9).

Furthermore, the restraints on the timing of adjustments must be taken into account (question 3, question 4).

Unfortunately, it is not possible to simply replace the previous SCCs in a contract with a reference to the new SCCs, as the new SCCs have to be "assembled" in a more elaborate way than before. Not only do the relevant Module(s) have to be chosen, but also various other options. Unlike the previous SCCs, the template for the new SCCs issued by the European Commission cannot be adopted in their entirety as part of the contract text; it is only a template that has to be adapted to the respective transfer scenario (question 12).

15. **Can several Modules be agreed between the same parties at the same time?**

Yes, this is possible. Clause 2(a) explicitly mentions the possibility of choosing several Modules.

Within a group of companies, it is common, for example, for a one company to act both as a processor and as a controller vis-à-vis another group company. These data flows were previously regulated in a single contract (IGDTA), which applied the applicable SCCs. Now, such an IGDTA will apply the applicable Module(s) of the SCCs.

16. **How are multiple parties to be dealt with? Is a separate IGDTA still needed?**

The new SCCs can be concluded by more than two parties at the same time. This was already possible and regularly utilized under the previous SCCs. The new SCCs now include the (optional) Clause 7, which explicitly regulates a later "accession" of further parties. The accession takes place by simply adding to the list of parties and adding another signature.

The provision in Clause 7 is unfortunately poorly drafted and not fully thought through. It states that a new party can only join with the consent of (all) other parties, but how this consent of the other parties is obtained and how it has to be expressed remains open. According to Clause 7, a unilateral declaration of intent by the new party is sufficient to become a party. This cannot seriously be the intention.

We therefore recommend waiving Clause 7 (it is optional) and, in relationships where the parties frequently change or are expanded, the accession or resignation of parties is regulated in a separate contract.

Such a separate contract can also regulate the procedure for adjusting the contract, as well as the bearing of costs, the exchange of information and other points that are not regulated by the SCCs. The new SCCs are therefore no substitute for an IGDTA.

17. **Can we continue to use our existing TOMS under the new SCCs?**

Yes, but they are no longer sufficient.

According to the title, Annex II of the Appendix still contains technical and organisational data security measures. However, the examples and also the SCCs require more than just data security measures. The TOMS under the new SCCs must also contain measures to implement and safeguard data subjects' rights and processing principles.

While this makes sense against the background of "privacy by design", it goes further than what is regularly provided for in today's TOMS. They must therefore include measures for data minimisation, data quality, storage limitation, accountability and data subject rights (the

examples in Annex II are limited to data portability and deletion obligations).

In addition, the explanations in Annex II state that the TOMS must be "described in specific (and not generic) terms". Most of today's TOMS in data processing agreements and SCCs are unlikely to meet this requirement, as they are usually written in a comparatively generic way on one to three pages. Annex II lists categories of measures (such as "measures for user identification and authorisation"), which must then be described in more detail. According to the explanatory notes, it must "clearly indicate which measures apply to each transfer/set of transfers".

18. Can we continue to use our previous descriptions of data transfers under the new SCCs?

Yes, but they are no longer sufficient.

The concept remains the same: Annex I.B of the Appendix describes the "transfer" and thus at the same time defines for which transfer of personal data or - formulated more broadly - for which processing activities the specifically agreed SCCs apply.

In this context, it has been common practice until now to include a very broad description of data transmissions in order to warrant that all were covered ("catch all"). This will probably continue to be the practice.

However, if a contract covers a multitude of (types of) data transfers, it will probably be expected in the future that they are listed separately from each other (e.g. in individual appendices or sections). The SCCs themselves state in an explanatory note to the Appendix that it must be possible to "clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the parties as data exporter(s) and/or data importer(s)". This is difficult to achieve with a "catch all" formulation.

On top of that, the list of information to be provided is more comprehensive than before. The following additional information is required:

- The special restrictions that are to apply to "sensitive data" (special categories of personal data). For such personal data, the SCCs require that additional measures be defined.
- The frequency of disclosure of personal data (one-off, regular).
- The retention period for the personal data or the criteria for calculating it.
- The "nature" of the processing (according to our understanding, this describes the operations such as collection, recording, modification, structuring, storage, retrieval, consultation,

disclosure, dissemination, interconnection, comparison, restriction, erasure, communication of personal data).

- In the case of processing, its duration and subject matter (which, however, already results from Art. 28(3) GDPR).

We assume that the descriptions of the individual transfers will, nevertheless, continue to be comparatively generic, as they primarily serve to record the parameters of the processing activities, but not to regulate them more closely in substance.

19. Which choice of law and which jurisdiction may and should we agree?

If the new SCCs are concluded to secure transfers of personal data under the GDPR, the law of a member state of the EEA (Clause 17) and a jurisdiction in the EEA (Clause 18) must be chosen - with the exception of Module 4 (Processor-Controller).

The chosen law must allow for enforceable claims by third parties, as the new SCCs provide third party beneficiary rights to data subjects; Clause 17 explicitly states this. Irish law, which is particularly popular with large online providers such as Microsoft, for example, did not previously provide for this, but has now been adapted specifically for the new SCCs by the time they come into force at the latest (but only for the new SCCs).

Which law is to be chosen within the EEA is not stipulated. In particular, it does not have to be the law of the exporter's place of business. This allows the parties to choose the law most favourable to them in relation to claims by data subjects in order to limit or impede their liability risk and claims for real performance. We are not yet in a position to assess which law is most suitable here.

This does not work with regard to jurisdiction, because this is not conclusively agreed. Even if one country is chosen as the jurisdiction, it will usually be possible to sue a party at its seat in another country if this appears more favourable. In any case, jurisdiction has no effect on actions by data subjects: the relevant provisions in Clause 18(a) and Clause 18(b) do not apply to them under Clause 3(a). Instead, Clause 18(c) applies, which establishes a non-exclusive place of jurisdiction at their habitual residence.

However, the entire provision of Clause 18 is unclear in that it only refers to the country, not the court district. Anyone wishing to sue must therefore first determine which court has local jurisdiction according to national procedural law. In our view, however, it is permissible to specify this court in Clause 18 - this only has an *inter partes* effect anyway.

If the new SCCs are only concluded for Swiss exports of personal data, Swiss courts and a Swiss jurisdiction may be chosen instead of the law

of an EEA country and an EEA jurisdiction. However, this is not required from Swiss law point of view. According to the CH DPA, it is only important that the contract is valid and enforceable as intended - even if this is done under foreign law and by foreign judges. It is only essential that their decisions are enforceable in Switzerland, which should not be an obstacle in the case of European courts.

If only the processor is subject to the GDPR (i.e. in the case of Module 4), one can choose any jurisdiction and any law (as long as it allows claims for third party beneficiary rights), which makes sense insofar as it can at least accommodate the controller (typically his client) on this point. Hence, if a hosting provider in the EEA has a client in the US, it will have to conclude the new SCCs (question 32), but it can at least subject them to US law and choose the US as the jurisdiction for disputes under the SCCs - if the client really wants this.

20. Does the reference to EU Member State also include a reference to Member States of the EEA only?

Yes, the GDPR is not only part of Union law, but also EEA law. The EEA consists of the EU and the EFTA member states without Switzerland (Iceland, Liechtenstein and Norway). The GDPR applies directly in these three countries. They are also not third countries from the EU's perspective. Therefore, where the SCC refers to "EU Member States", it also means member states (only) of the EEA.

21. What applies with regard to the UK?

For transfers of personal data to the UK, the new SCCs will not be required from either an EEA or Swiss perspective, as the UK is considered a whitelisted third country.

The new SCCs do not apply to exports from the UK to non-whitelisted third countries, i.e. they may not be used in these cases. For such exports, the old SCCs must still be used, which is particularly important in the case of renewal of IGDTAs if they are also to cover exports from the UK, as is often the case.

The practical solution here is that new IGDTAs only supersede existing IGDTAs to the extent that they do *not* concern transfers of personal data from the UK to non-whitelisted third countries. Until a new solution is also available for the UK, this approach means that there are two parallel contracts, which in our opinion makes more sense than concluding a combined, but very complicated IGDTA - only to have to adapt it again before long.

Meanwhile, the UK's data protection authority, the ICO, is working on its own SCCs, which it plans to present in draft form in the summer (2021). According to reports, they differ significantly from the new SCCs of the European Commission, which will complicate multinational

data protection contracts such as IGDTA considerably if the ICO does not also recognise the EU's SCCs as an alternative.

22. What if we don't like a clause in the new SCCs?

Clause 2(a) clarifies that the SCCs must be adopted unchanged and in their entirety unless they themselves provide for optional provisions or offer choices. The SCCs may be embedded in a more comprehensive contract (e.g. an IGDTA or a provider contract), but this other contract may not directly or indirectly contradict the provisions of the SCCs or restrict the rights of the data subjects. Clause 5 states that the provisions of the SCCs take precedence over such a contract.

In the coming months there will undoubtedly be discussion about the extent to which additions or clarifications to the SCCs are possible. From our point of view, these are permissible and even necessary from a practical point of view (see question 23).

Even if the SCCs themselves must be adopted unchanged, adjustments are nevertheless conceivable in certain exceptional situations:

- This applies to cases in which the SCCs are used for scenarios for which they were not intended, such as data transfers between parties located in the EEA or in whitelisted third countries, or data transfers that are not subject to the GDPR. See also question 7. In particular, in an IGDTA, a set of contractual clauses may also need to govern data transfers from other jurisdictions with data protection laws for which the SCCs need to be slightly adapted. In such cases, the SCCs can be adapted. The unamended adoption only applies where they are to be relied upon as contractual safeguards under Art. 46(2)(c) GDPR. Even where the clauses are used as a data processing agreement, they may be modified (but whoever does so can no longer rely on the recognition under Art. 28(7) GDPR).
- Amended SCCs can, at least in theory, be approved by a competent EEA data protection authority (Art. 46(3)(a) GDPR).

The immutability of the SCCs (and also of the SCCs-DPA) is makes sense: Tthey are not merely aids to contract drafting, but are considered sufficient for the purposes of Art. 46 GDPR and Art. 28 GDPR, even if they should not substantively so. This means that they must be used as authorized.

23. Can we supplement and clarify the SCCs with our own regulations?

Yes, this is possible, but it must be done through a separate contract and such regulations must neither weaken the protection intended by the SCCs nor contradict them. Clause 5 additionally states that in the event of contradictions, the provisions of the SCCs prevail.

While the SCCs may not be amended as such and may not be overridden by other provisions, they may be part of a wider contract, as Clause 2(a) explicitly states. Such a contract may well include data protection issues.

These can be, for example, additional aspects that are not or only incompletely regulated in the new SCCs (such as the consequences of rejecting a sub-processor), but also implementing provisions (such as the way in which the instructions of the responsible person towards the sub-processor are determined, which will be particularly important for providers of standardised services).

It is essential with regard to such clarifications and implementation rules that they do not adversely affect the data protection of the data subjects and do not weaken the SCCs in their (data protection) effect.

That said, we believe that it must be permissible for the parties to allocate risks or tasks between themselves that are not regulated in the SCCs - i.e. what happens if a new sub-processor is rejected or the sub-processor does not want to implement an instruction because it does not fit into his service concept. It must also be permissible to restrict the exercise of rights under the SCCs for non-data protection purposes (on liability and the possibility of restricting it, see question 38). Moreover, it must be permissible to further restrict the data importer's processing options or to prohibit it in certain situations. Although the SCCs provide for the disclosure of personal data, it must for example be permissible to contractually agree that the importer will not disclose the personal data received - not even to sub-processors. This contradicts the SCCs, but not their protective purpose. From this point of view, the only cases in which the SCCs may not be contradicted is when this would run counter to their protective purpose. In our view, however, a restriction according to which on-site audits of the exporter must be mandatorily and completely delegated to a third party, as cloud providers regularly provide today (question 28), is problematic.

For the adjustment of the SCCs in the case of joint controllers, see question 27

24. **Do the new SCCs have to be adapted for use under the CH DPA? How do we use them under the CH DPA?**

The new SCCs can also be used as they are for the purposes of the CH DPA and, in our view, ensure the "appropriate data protection" (Art. 16 question 2 revised CH DPA).

The SCCs initially refer to the GDPR around 45 times. However, the references do not lead to a relevant weakening of the protection of data subjects whose data is processed in Switzerland and are to be exported with the help of the SCCs. In our opinion, this also applies in the following cases:

- The transfer of personal data is permissible, for example if the recipient's country offers adequate protection from the perspective of the GDPR, but not from the perspective of Switzerland. However, this hardly ever occurs. This difference seems negligible to us (it currently only affects Japan), since it is not necessary to ensure the same protection as under the CH DPA, but merely a suitable protection.
- In the event of a data breach, the processor only has to support the controller in fulfilling its obligations under the GDPR, not under the CH DPA. The basic obligation (the notification to the controller) exists independently of this. Therefore, this is sufficient.
- In the event of a request from a data subject, the processor only has to assist the controller in fulfilling the data subject's rights under the GDPR, not the CH DPA. However, since the processor is required to follow his instructions anyway, this is sufficient.
- With regard to the designation of the competent supervisory authority, Clause 13 ("Supervision") does not provide for a text that completely fits the FDPIC, but all variants refer to Annex I.C, where the "FDPIC" can be agreed as the "competent supervisory authority". This is undoubtedly a valid contractual agreement, even if the FDPIC has no function under the GDPR. Which variant is chosen in Clause 13(a) is therefore irrelevant for the CH DPA (it is only relevant if the GDPR is applied in parallel). The term "competent supervisory authority" is used in around 14 places in the SCCs, for example in the obligation to report data security breaches.

There are around 17 references to "Member State". In principle, the references do not affect the required level of protection. They primarily serve to determine the applicable law and jurisdiction. The previous SCCs already used the term "Member State"[12] for this purpose and did not even provide for a jurisdiction, which did not negatively impact their suitability. In the new SCCs, too, it is left to the parties to designate the applicable law (Clause 17); in addition, there is the designation of a (non-exclusive) jurisdiction (Clause 18). If the parties agree on Swiss law and a place in Switzerland as the jurisdiction, this should be considered as agreed, even if the pre-printed clauses state that the designated jurisdiction must be the court of an "EU Member State". The true intention of the parties prevails here as well. The same applies with regard to the choice of law, whereby in this case "Option 1" of Clause 17 must be chosen.

---

12 See for example Clause 9 of the Processor Model Clauses of 2010: "The Clauses shall be governed by the law of the Member State in which the data exporter is established, namely ....".

If the choice of law is made for Switzerland, the reference in Clause 11(e), which leads nowhere, should not harm the protection of the data subjects and thus third party beneficiaries, because their right to sue arises from the contract and the enforceability of a judgment from the jurisdiction of the Swiss court. Clause 18(c) also gives the data subject a right to sue in an EU court if he or she is habitually resident there. As Clause 18 does not provide for any of the jurisdictions to be exclusive, it remains possible to bring an action against a Swiss party at its seat or domicile in Switzerland.

In practice, however, the question arises as to whether Swiss law and a jurisdiction in Switzerland must be chosen. In accordance with previous practice, this is not the case. It is perfectly permissible to instead agree on the SCCs under the law of an EU member state and under the jurisdiction by a civil court in an EU member state. This will even be the norm if the new SCCs are concluded in cases where one contract must cover data transfers from several European countries.

As a result, the new SCCs can be used unchanged both for purely Swiss data exports and for mixed EEA and Swiss data exports, provided that in the case of data exports from Switzerland Annex I.C contains a reference to the FDPIC as the "competent supervisory authority" for data exports from Switzerland (and in the case of a mixed data export also a reference to an EEA data protection authority for data exports subject to the GDPR). This is the approach we recommend.

It may at first glance seem obvious but nevertheless is not recommended, to supplement the SCCs with a clarification that in the case of data transfers from Switzerland, all references to "Regulation (EU) 2016/679" (= GDPR) are deemed to be a reference to the CH DPA; all references to specific articles of the GDPR are deemed to be a reference to their corresponding provision in the CH DPA; and all references to the EU are deemed to be references to Switzerland. This may seem to make sense from a Swiss perspective, but may come into conflict with the GDPR where a data transfer from Switzerland is subject to the GDPR in parallel. In this case, the SCCs must apply unchanged in order to be effective. Therefore, if such an adjustment is made, it would have to be made clear that this adjustment only applies to data transfers from Switzerland insofar as they are subject to the CH DPA, with the original wording of the SCCs taking precedence in the event of conflict.

Since such adjustments (as mentioned) are in substance unnecessary anyway, they should be dispensed with for the sake of simplicity.

Pro memoria: The description of the data transfer in Annex I.B of the Appendix must be worded in such a way that Swiss data exports are also covered. This is because Annex I.B ultimately defines the subject matter of the specifically agreed SCCs. This adjustment can be

particularly important in the case of SCCs concluded at European level, because Switzerland tends to be forgotten in these cases if it is not realised during the drafting process that Switzerland is not part of the EEA.

25. Does the use of the new SCCs have to be reported to the FDPIC?

Yes, the use of the new SCCs must be reported to the FDPIC in accordance with Art. 6(3) CH DPA, at least if it is used in the sense of Art. 6(2) CH DPA to safeguard the disclosure of personal data to an non-whitelisted third country. Whether a simple letter is sufficient or the clauses must be submitted to him with appropriate additional information depends on whether and in what form he will recognise them under Art. 6(3) CH DPO. It can be assumed that he will recognise them in one form or another, but he has not yet expressed his opinion.

Under the revised CH DPA, notification will only be necessary if the SCCs are used in a version that is not recognised by the FDPIC (e.g. with unrecognised adjustments). For most cases, therefore, the obligation to notify will no longer apply under the revised CH DPA.

26. What special features have to be considered for a Controller-Controller transfer (Module 1) under the new SCCs?

If a controller receives personal data under the SCCs, it is no longer subject to only some general processing principles as was the case before. The new SCCs formulate the requirements for it as an importer rather in detail. The following points are worth particular emphasis:

- The importer may use the data received for fewer purposes than a controller would be allowed to under the GDPR (Module 1, Clause 8.1). Care must therefore be taken to ensure that the purposes listed in the Appendix of the SCCs are sufficiently comprehensive. After all: the recipient is still allowed to use the data for official or judicial proceedings. Also, the parties are of course free to adapt the Appendix and thus also the listed purposes at any time. The importer is therefore likely to reserve the advantage of the right to demand such adjustments.
- The importer must inform data subjects of its name and contact details, the categories of data transferred and any further recipients, the purpose of such onward transfers and the legal basis under the SCCs (Module 1, Clause 8.2(a)). The SCCs provide that this information can also be provided via the exporter (and its privacy statement), but the exporter has no obligation to provide this information. If the importer can show that it would be disproportionate for it to inform the individual data subjects itself, then "public" information should suffice. In other words, a controller in a non-whitelisted third country will

have to publish at least a privacy statement on its website under the SCCs.

- The regulation on dealing with incorrect or out-of-date data goes beyond the obligations set forth by the GDPR. The SCCs provide that the two controllers must keep each other informed about corrections in their data files as far as they concern the transferred data (Module 1, Clause 8.3(b)).
- If a breach of data security occurs that has relevant risks for the data subjects, the importer must now not only inform the exporter, but must also directly contact the relevant data protection authority that the parties designated in accordance with Clause 13 (Module 1, Clause 8.5(e)), and if necessary also the data subjects. The exporter does not have to submit a report, but may have to support the process.
- The importer is obliged to keep a log of data security breaches, also for those that were not reported (Module 1, Clause 8.5(g)). The CH DPA does not provide for such an obligation. However, the SCCs also go further with regard to the remaining documentation obligation: The importer is contractually obliged to document its processing activities and must allow the data protection authority to inspect them upon request (Module 1, Clause 8.9).
- The onward transfer of personal data by the importer is regulated more flexibly under the new SCCs than under the previous SCCs. Of course, it is possible when SCCs are adopted, but now disclosure is also possible in the context of official and judicial proceedings where the conclusion of SCCs is not possible (cf. question 43). The use of amended SCCs is also possible in these cases, unless the importer is subject to the GDPR.
- The rights of data subjects are specifically regulated: Data subjects have the right to information, correction and deletion as well as the right to object to the use of their data for marketing purposes. They can assert these rights directly against the importer. The right to information also includes a claim for the names of the third parties to whom the importer has disclosed the data, which means that information about them must be recorded. This also goes beyond the CH DPA. Restrictions on data subject rights are possible, but the SCCs do not specify what these restrictions are: They only state that the importer may refuse if this is (i) permitted under the law of the "country of destination" and (ii) necessary to protect the (overriding) rights of other persons (including the controller) or the other objectives[13] listed in Art. 23(1) GDPR. The term "country of

[13] In addition to the protection of the data subject and rights of third parties, these are national security, national defence, public safety, the prevention, investigation and detection or prose-

destination" is not clear at first glance, but means the country the importer, as becomes clear when looking at Clause 15.1(a), where the term is also used and further explained. If the importer's home country does not regulate the right to information, this sub-clause does not prevent a refusal to provide information, i.e. in practice, information can in principle be refused if other overriding interests prevent it.

Unlike under Art. 13 f. GDPR, it is no longer sufficient under the new SCCs for parties to simply offer data subjects a link to the SCCs in the privacy statement. Data subjects now have the right to inspect the specifically agreed SCCs including the Appendix (Module 1, Clause 8.2(c)). While business secrets and personal data may be redacted, a meaningful summary must be provided instead if this is necessary for assessing the lawfulness of the arrangement. In other words, the data flows must be made transparent, which goes beyond the normal duty to inform and the right of access under the GDPR. However, there is no requirement that the privacy statement must specifically include an offer to provide the copy of the SCCs; the data protection statement can therefore remain as it is in this respect, with the exception of updating the link to the new EU SCC.

On the question of enforcement and liability, c.f. questions 37 and 38. On new information obligations, c.f. question 35**.** On disclosure to authorities, c.f. question 40. On special issues in the case of joint responsibility, c.f. question 27

27. What applies in the case of disclosure to a joint controller in a non-whitelisted third country?

Transfers of personal data between joint controllers must also comply with the requirements of Art. 44 et seq. GDPR and Art. 6 CH DPA. The SCCs can therefore also be concluded between joint controllers. In this case, Module 1 (Controller-Controller) is used.

Whether the distribution of responsibilities between the joint controllers, as provided for in the SCCs, is suitable for the specific case at hand must be assessed on a case-by-case basis. In the majority of cases, this SCC will fit, because if a data controller subject to the GDPR (or the CH DPA) is jointly responsible for data processing with a company that is not legally obliged to comply with data protection, it will want to conclude a regulation similar to the SCCs out of pure self-interest, in order to at least be able to have recourse to the other joint controller(s) in the event of a claim.

---

cution of criminal offences, the protection of other important public interest objectives, the protection of judicial independence and judicial proceedings, the prevention, detection and prosecution of breaches of professional ethics, the exercise of official authority and the enforcement of civil claims.

Because the SCCs regulate the responsibilities between the parties in all areas relevant to data protection, they can, in our opinion, meet the requirements of a contract under Art. 26 GDPR if their regulatory content (coincidentally) fits the situation in question. If this is not the case, we believe that it must be permissible to create an additional set of responsibilities in addition to the SCCs, which impose additional obligations on one or the other party. This may at first sight formally contradict the rules of the SCCs but it will be permissible as far as the protective purpose of the SCCs is achieved.

If, for example, a data breach occurs, the importer is obliged under the SCCs to report this breach to the competent supervisory authority (Module 1, Clause 8.5(e)). Here, in our opinion, it must be permissible in the case of joint data processing to agree that this data breach notification is instead made by the exporter on behalf of all controllers, which in practice is probably the most sensible course of action anyway, as it is closer to the supervisory authority. Those who want to be particularly cautious will not only state in the supplementary contract between the joint controllers that the exporter is obliged to report, but in addition that it also does so on behalf of the importer. In this way, it can be argued later that the importer has nevertheless fulfilled its obligation under Module 1, Clause 8.5(e) of the SCCs. In such cases, it will be necessary to make an additional provision for the purposes of Art. 26 GDPR.

28. What special features have to be considered for a Controller-Processor transfer (Module 2) under the new SCCs?

This scenario occurs particularly often in practice and will also be the most debated. For the processor, the new SCCs are comparatively disadvantageous. In a data processing arrangement within the EEA or in a whitelisted third country, only the requirements as per Art. 28(3) GDPR or of the even less strict CH DPA must be observed. Under the SCC, however, more detailed and stricter rules apply – and they can't be changed. At least there is a possibility of partially avoiding these disadvantages (question 30).

The following points are to be emphasised:

- While Art. 28(3)(a) GDPR only requires that the processor may only process data on "documented instructions from the controller", the SCCs additionally require that they can be changed at any time during the term of the contract. This will be a challenge for providers of standardised services, as they usually agree with the client that the contract and the configuration of the client's services are the client's "final and conclusive" instructions. At first sight, this is contrary to the new rule. However, it can be argued that the ability to customise the configuration of the services must satisfy the required customisation ability of the SCCs, as it is self-evident that

instructions need only be followed to the extent that they are within the scope of the services. If the instructions are not followed, the controller has an extraordinary right of termination, also of the main contract, as a result of the new SCCs. It remains to be seen to what extent this can be used as a right to terminate the contract at any time without cause by the controller issuing an instruction to the processor which the latter is not prepared to implement and the contract is then terminated on the basis of Clause 16(a)-(c).

- In addition to the obligation to process data in accordance with instructions, the SCCs prohibit the processor from processing the data for purposes other than those specified in Annex I.B. of the Appendix. In practice, it must be ensured that if the processor also wants to be able to process personal data for his own purposes (as the controller) (e.g. for the purpose of anonymisation for his own purposes or for the purpose of disclosure in official or judicial proceedings), this must also be stated in Annex I.B.
- The processor is obliged to inform the controller if it becomes aware that the personal data he is processing is incorrect or out of date. This obligation goes beyond the obligations of a processor under Art. 28 GDPR. After all, the processor has no duty to search for incorrect or outdated data so it can take advantage of pursuing a head-in-the-sand policy.
- The obligation to return personal data does not go as far as per the GDPR. According to Art. 28(3)(g) of the GDPR, the only condition under which a processor is not obliged to return data after the end of the contract is if the law of the EEA or a member state prohibits it from doing so. In Module 2, Clause 8.5, the data processor can refer to his domestic law - which has already been the standard in practice. Correctly, it is also stated that as long as deletion has not taken place, the data must continue to be protected. This rule is missing in many data protection agreements today.
- With regard to technical and organizational measures (TOMS), a duty is imposed on the processor to regularly check their adequacy (Module 2, Clause 8.6(a)). Many processors want to transfer this duty to their client with the argument that only the client knows its data and can judge how far protection should go. In our opinion, it is still possible to proceed in such a way that the processor presents his measures (i.e. the TOMS) to the client and the client must confirm in the main contract that these are sufficient in view of his personal data and processing activities. This must be repeated during the term of the contract, as it is inherently the responsibility of the processor to verify their adequacy.

- It should also be noted that the TOMS no longer only have to contain measures for data security, but also measures for compliance with the data subjects' rights and the other processing principles (Module 2, Clause 10(b)). This was not the case previously. They must therefore be supplemented (question 17). They may also have to be more detailed than before.
- Of course, the processor is obliged to report breaches of data security (Module 2, Clause 8.6(c)). Here, however, it is noticeable that no maximum time limit is provided for (only "without undue delay").
- Although the SCCs provide for a general duty of assistance of the processor towards the controller (Module 2, Clause 8.6(d)), this is worded less specifically than required by Art. 28(3) GDPR. However, since the SCCs also qualify as approved data processing agreement clauses under Art. 28(7) GDPR (see question 44), this is not relevant.
- Unlike before, the new SCCs also regulate the onward transfer of data to third parties. As far as sub-processors or official or judicial proceedings of the controller are concerned, this does not seem to be a problem. A stumbling block, however, is the case of onward transfer requested by the controller, i.e. where, for example, the client requests his provider to disclose the data to any third party. According to Module 2, Clause 8.8, the instruction is not sufficient in this case. One of the four cases according to Module 2, Clause 8.8 must also be fulfilled. It is not clear whether it is the controller who must ensure this or the processor. Presumably, it will be the latter who will pass the ball back to the controller by requiring it in the main contract to order the disclosure of personal data only if and when the requirements of Module 2, Clause 8.8 are met (the SCCs do not, however, impose on the controller the obligation to only issue instructions that are permissible under the SCCs).
- The processor must "document" its processing in an appropriate manner for the controller (Module 2, Clause 8.9(b)). It is unclear what this exactly means. The obligation goes beyond Art. 28(3)(h) GDPR, according to which a processor must only be able to document that it complies with the requirements of Art. 28 GDPR (and the data processing agreement). The latter obligation is included separately (Module 2, Clause 8.9(c)).
- The right to audit is also specified in more detail than provided for in Art. 28(3)(h) GDPR. The complete delegation of the audit right to a third party commissioned by the processor (as cloud providers regularly provide today) is not envisaged; it is merely stated in favour of the controller that it may also rely on "certifications" of such third parties in its decision to conduct an

audit (Module 2, Clause 8.9(c)). Conversely, it follows from this wording that the right to audit may not be waived in its entirety. That said, Module 2, Clause 8.9(d) states that the responsible person is permitted to call in an independent auditor. It will thus be permissible for a processor to require that its client first exercise its audit rights on the basis of existing audit reports (or certifications, which is not the same thing) and, only if this is not sufficient, to mandate an independent (but specified by the processor) third party to carry out the audit (i.e. the client never carries out an audit on site itself).

- The involvement of sub-processors is possible in analogy to the regulation provided for in Art. 28 GDPR; it gives the processor a surprising amount of freedom:
  - The SCCs provide that both the individual authorisation procedure and the blanket authorisation procedure have a right of appeal. The SCCs do not specify a notice period; depending on the case scenario, it is likely to be between 10 and 180 days.
  - What the SCCs do not regulate are the consequences of an objection, i.e. whether the controller must terminate, the processor may terminate or is simply prohibited from using the new sub-processor. The rule that the SCCs must be interpreted in conformity with the GDPR means that it is not permitted to provide for the involvement of a sub-processor unless the controller has a (feasible) option to exit in case of an objection.
  - The SCCs provide that a sub-processor is bound in a serial manner, i.e. it has a contract only with the processor, not with the controller. However, the contract between the processor and the sub-processor must be made available to the sub-processor on request (business secrets may be redacted) (Clause 9(c)). The only claim that the controller must be granted directly against the sub-processor is the right to terminate the sub-processing (i.e. the contract between the processor and the sub-processor) and to demand the return or deletion of the data - if the (intermediary) processor goes bankrupt or is no longer capable of acting (Clause 9(e)). This is a somewhat strange provision, because the obvious solution would have been for the controller to be granted a right to enter into the contract, but the provision is better than nothing.
  - Somewhat illogical is the provision in Clause 9(d), according to which the processor is liable for the sub-processor's compliance with its contract with the processor, but not for the sub-processor's conduct in general, which would be the

usual practice. If the processor concludes an unfavourable contract with his sub-processor, it thereby limits his own liability. The processor is not explicitly obliged to conclude the SCCs with the sub-processor; it is sufficient that the contract provides for the same data protection obligations in substance (Clause 9(b)).

- If a controller wishes to have direct contractual relationship with the sub-processor, it must make it a direct processor, which is permissible but not required.

Unlike under Art. 13(f) GDPR, it is no longer sufficient under the new SCCs for a controller to offer data subjects a link to the SCCs in its privacy statement. Data subjects now have the right to inspect the specifically agreed SCCs including the Appendix (Module 2, Clause 8.3). This should not be a problem for commercially commissioned processors, as their SCCs are usually generally available anyway. Nevertheless, the obligation to disclose the SCCs can also lead to an obligation to disclose the names of the processors commissioned by a company in non-whitelisted third countries. A data subject can basically demand that a company produce all SCCs with processors in non-whitelisted third countries and enforce this claim in court (insofar as the new SCCs have been agreed).

On the question of enforcement and liability, c.f. questions 37 and 38. On new information obligations, c.f. question 35. On disclosure to authorities, c.f. para 40

29. How should we proceed if we contract a service provider for ourselves and for other group companies?

If the service provider is a processor and is located in a non-whitelisted third country, the SCCs will have to be concluded with it for two of the four Modules. This is because the company that uses the services of the processor for itself will be considered controller, whereas it will act as a processor if it procures the services on behalf of its group companies (unless it concludes the contract with the service provider on behalf of all group companies, which a service provider would normally not want to do). For the first case, Module 2 applies, for the second case Module 3.

If the processor intends to process personal data also for its own purposes or as a controller (e.g., user data), then even Module 1 needs to be agreed.

30. How can a processor protect itself from the disadvantages of the new SCCs at least in relation to the client?

The "need for protection" arises because many of the new provisions of the SCCs are not only disadvantageous for the processor (question

28), but it also cannot change them because they provide that they may not be adapted.

In order to nevertheless protect itself, we recommend to make use of a party in the EEA or a white-listed third country such as Switzerland as the contracting entity. The controller (e.g. client of the cloud provider) concludes his contract with the "local" processor and is therefore not forced to agree on the SCCs. He can agree on a less extensive data processing agreement. The SCCs do come into play, but only in the second stage, when the local processor passes on the client's personal data to its foreign group companies for processing. These are then sub-processors and the SCCs must be concluded with "Module 3 (Processor-Processor)".

It is not required under the GDPR (nor under the CH DPA) that the controller concludes a direct contract with the sub-processor; the SCCs do not provide for such direct contractual relationships either, but only for a right of subrogation in the event of a default by the processor (Module 3, Clause 9(e) of the "Processor-Processor" Module).

We expect that many service providers will choose this route to protect themselves. Even though their customers will not be responsible for entering into the SCC in these cases, they of course remain responsible for the processing as such. Therefore they will nevertheless have to make sure that their service provider will enter into the SCC and will comply with them.

31. What special features need to be taken into account if a processor wants to use a sub-processor in a non-whitelisted third country?

A distinction must be made here between where the processor is in Switzerland or where it is subject to the GDPR:

- If one or the other is fulfilled, then it will use the SCCs because the transfer restrictions under Art. 44 et seq. GDPR and Art. 6 CHA DPA apply in the same way as they do to a data controller (with the exception that under Art. 6(3) CH DPA, it is generally not obliged to notify the FDPIC if it is not the owner of the data collection).
- If the processor is located in a non-whitelisted third country and is not subject to the GDPR (which may be unclear: Clause 7), it does not have to use the SCCs for the involvement of a sub-processor under either the CH DPA or the GDPR, but may do so. If it has signed the SCCs itself, the less strict requirements of Clause 9 apply to the involvement of a sub-processor, according to which his contract with the sub-processor must only (but still) ensure the same level of protection as the SCCs, but the SCCs no longer have to be used for this purpose (see question 31). In

practice, however, the SCCs or a derivative thereof are likely to be used in most cases.

- Finally, the case in which a processor of a controller transfers some data to another processor of that controller must be distinguished from both the above cases. This case is not covered by Module 3, because Module 3 assumes a relationship of subordination between exporter and importer, i.e. the latter is the sub-processor of the former. For this special case, nothing at all will have to be agreed between the two processors, as long as the controller has concluded the SCCs with both processors separately (according to Module 2).

The first case is regulated by the SCC with the third Module 3 (Processor-Processor). Attention must be paid to how the SCCs regulate the "chain of command". Here, too, the serial approach is used, i.e. the instructions and communication run via the processor, who represents the controller (up to now, the Controller-Processor SCCs were used analogously for these cases). The processor is granted the right to issue additional instructions to the sub-processor (Module 3, Clause 8.1(b)), but the processor must warrant the sub-processor that it has imposed the same obligations on it as those that were already imposed on itself by the controller (Module 3, Clause 8.1(d))[14]. In practice, this is only relevant if the sub-processor is prosecuted because the processor gave it too much freedom.

If the SCCs are used with the third Module 3 (Processor-Processor), the explanations for Module 2 (Controller-Processor) apply analogously (section 28). In contrast, the case of a breach of data security must be mentioned, in which case the sub-processor must inform not only its direct contractual partner, the processor, but also the controller "where appropriate and feasible" (Module 3, Clause 8.6(c)). However, the sub-processor only has a duty of cooperation towards the processor. Direct notification by the sub-processor to the controller is probably only appropriate in exceptional cases; this has an effect on how quickly the controller learns of a data breach. After all, the sub-processor also has a duty to the controller to deal with any requests appropriately (Module 3, Clause 8.9(a)). A direct right of audit is not provided for; this is the responsibility of the processor.

The involvement of further sub-processors by a sub-processor is not clearly regulated (Clause 9). Such a chain of processing is provided for under the SCCs, but according to the SCCs, the approval to use a sub-processor must come from the controller and not from the processor. Although this principle is understandable, it is designed in a way that is

---

[14] This wording also makes it clear that the authors of the SCCs were only thinking of the case where there is *a* processor in the EEA or in a whitelisted third country and the processing "chain" is continued, at the latest from the first sub-processor, in a non-whitelisted third country. Of course, this does not have to be the case, but it is probably irrelevant in practice.

out of step with actual practice. First of all, it is clear that it must ultimately be the controller who decides on the involvement of processors or sub-processors. This already follows from Article 28 GDPR: The controller should and must have some control over who processes his data - whether this processor is formally the first or only the second or third link in the chain. What is unrealistic in practice is that the sub-processor - i.e. the contractual partner of the processor - must contact the controller (i.e. the client of the processor) directly and inform the controller that it is about to use another party as a sub-processor. In other words: The SCCs requires a circumvention of the official reporting lines. Since in the end it can only be a matter of the controller finding out about the involvement of another party and agreeing to it or not objecting to it, the processor will agree with his sub-processor that the duty to inform the controller is delegated to the processor (as the direct contractual partner of the client) in the cases prescribed by the SCCs.

These questions are certainly of practical relevance. Let's take the example of a European SaaS provider, which in turn uses a cloud instance of Microsoft or Amazon for its service. The clients of the SaaS provider will conclude a data processing contract with the provider according to Art. 28 GDPR, and the provider in turn will conclude a data processing contract with Microsoft or Amazon. The European Microsoft and Amazon companies will - as processors - conclude the SCCs with Module 3 (Processor-Processor) with their US group companies. In the case of Microsoft, this will be Microsoft Corp., which in turn will involve other Microsoft companies as sub-processors. According to the SCCs, the latter must be correctly submitted by the sub-processors of Microsoft Corp. to the clients of the SaaS provider for approval. Microsoft already handles this in such a way that it merely provides a list of all the companies involved by making it available on the internet. The SaaS provider will correctly ask his client not only to approve the involvement of Microsoft or Amazon, but also to approve their list of sub-processors by reference to the list. This should satisfy the SCCs.

32. Does a processor in Switzerland or the EEA also have to conclude the SCCs with its clients in non-whitelisted third countries?

Yes, unless the (re-)export of the personal data cannot be otherwise secured or justified. This need to govern this scenario has been ignored in practice in most cases so far. An example is a hosting provider in Switzerland who serves a client in the USA. These cases occur frequently, especially in corporate groups, when a European group also operates the IT infrastructure in Europe for non-European group companies.

Legally, it has always been argued in that these cases - if at all - the data subjects would have consented to the processing in the controller's country and thus a re-export to this country is covered by their consent (e.g. Art. 49(1)(a) GDPR). This also makes sense: anyone who is hired by a US company as an employee assumes that the HR data will be processed in the US and also consents to this. There is no reason why this personal data, if it happens to be stored on a server in Europe instead of in the USA, should not be transferred back to the USA. The problem with this line of argument is that consent is required on a case-by-case basis, or even explicit consent depending on the type of data (under the CH DPA), but such consent is often lacking. This fact was overlooked because the rights of the data subjects are not at risk and there were no approved SCCs for this case under the GDPR. Instead, Controller-Controller SCCs were used in some cases.

The new SCCs now also cover this case with Module 4, which means that they must now be consistently adopted in the cases in question. This applies in particular to intra-group IGDTAs, where such data flows occur regularly.

The provisions of the new SCCs on this case scenario do not go very far. Essentially, the entity in the non-whitelisted third country undertakes vis-à-vis its processor (i) not to prevent the latter from complying with the GDPR, (ii) to ensure adequate data security with the latter, and (iii) to assist the latter in fulfilling requests under the GDPR. These are innocuous obligations.

The rights in favour of data subjects, which are constituted by the conclusion of the SCCs, are much more important: They should presumably be able to take action against the client of the processor if the latter is instructed by the client to carry out a data processing that is inadmissible under the GDPR and thus itself violates the GDPR. In these cases, the client is also liable to the data subjects without limitation (question 36).

Therefore, as long as the client of a processor who is in the EEA or Switzerland or otherwise subject to the GDPR allows the processor to ensure adequate data security and does not require the processor to carry out any unauthorised data processing, the conclusion of the SCCs will not be particularly problematic. The client will even get additional rights to make a damages claim against its processor, which it would not have without the SCCs. If, on the other hand, the client wants to use the data processor for data processing that is not permitted under the GDPR (or the CH DPA), the SCCs will expose the client to considerable risks. In these cases, not only does the processor have a liability claim against its client should the latter's conduct get it into trouble as a processor (many provider contracts already contain such a provision today). The SCCs also give data subjects a legal instrument to take direct action against the client (question 36). This has not been

the case so far and is likely to be a significant competitive disadvantage for European providers.

However, Module 4 offers a small advantage over the other Modules: In the scenario discussed here, the parties are free to choose the law and to agree on the jurisdiction as long as the chosen law allows claims enforceable by third parties (question 19; Clause 17 and Clause 18). The client's domestic law and courts can therefore be chosen.

33. What happens if the sub-processor is in Europe, but the processor is in a non-whitelisted third country?

The European Commission has not thought of this case, although it can certainly occur in practice - for example, if a provider in the US has data centres operated by subsidiaries in Europe, but concludes its customer contracts itself. The customers do not have to be subject to the GDPR.

Strictly speaking, the new SCCs cannot be used in these cases under Art. 46(2)(c) GDPR, as none of the modules fit this scenario. One solution would be BCRs, but where they are not available, it must either be ensured that no access to the data from a non-whitelisted third country is possible on the part of the processor (and thus there is no transfer relevant under Chapter V of the GDPR) or the SCCs are applied by analogy in a risk-based approach.

In the latter case, we recommend using Module 4, but not with the controller, but with the processor as its *indirect* agent: Formally, the processor concludes the contract with his sub-processor, but in substance he represents his client - the controller - by ultimately carrying out the controller's instructions and data processing. This corresponds to the practice under the old SCC, according to which the SCC for controller-processor transfers were used analogously for processor-sub-processor transfers. This was also generally accepted: The processor acts as if he were the controller and the sub-processor as if he were the processor.

The procedure must be different, though, where the processor in the insecure third country has a controller subject to the GDPR and has therefore concluded the SCC with him in accordance with Module 2. In this case, the sub-processor provisions set forth in Clause 9 apply and the processor will have to conclude the SCC according to Module 3 with its sub-processor or another back-to-back contract that essentially corresponds to Module 2. The reason: In this case, the processor is already bound to comply with data protection via his contract with the customer (i.e. the SCC according to Module 2); the use of Module 4 is unnecessary and - in view of Clause 9 - would also be insufficient. Insufficient - again because of Clause 9 - is an ordinary data processing agreement according to Art. 28(3) GDPR, although the sub-processor

is located in the EEA or a secure third country. The Commission has not considered this scenario either.

34. Do we also have to secure internal transfers to non-whitelisted third countries with the SCCs?

Yes, but this is a blind spot in both the GDPR and the CH DPA and has not been addressed in the literature. This refers to transfers of personal data within the same legal entity to non-whitelisted countries without adequate data protection (e.g. to a branch office).

Legally, it can be argued in these cases that if the controller or processor is itself subject to the GDPR or the CH DPA (because its headquarter is in the EEA or Switzerland), this also applies to those parts of its operations that are located in a non-whitelisted third country. This means that it must also comply with the provisions of the GDPR and the DPA there. To ensure this, it must take appropriate technical and organisational measures (TOMS). The latter include appropriate instructions, training and controls with regard to the employees who process the personal data for it in the non-whitelisted third countries. Under the GDPR, this results from Art. 25, 29 and 32 GDPR. Under the CH DPA, this results from Art. 7 CH DPA and in future from Art. 7 and 8 revised CH DPA. The problem of access by foreign authorities naturally arises here to the same extent as in the case of transfers to third parties, and ultimately also requires the same assessments and measures (question 40).

However, the SCCs do not have to be concluded in the technical sense of the word. Legally, this is not even be possible, because a company cannot enter contracts with itself.

In the case of an IGDTA, however, it has proven useful in practice to impose the SCCs analogously on branches in non-whitelisted third countries - not as a contract, but as an internal instruction. Branches can thus be included in such an IGDTA as independent parties, whereby it should be made clear in a clause how the provisions of the IGDTA are to apply in their case.

35. Are there any new information obligations towards data subjects under the new SCCs?

Yes, in two respects:

- For controllers in non-whitelisted third countries, the SCCs provide for an information obligation vis-à-vis data subjects, but that obligation does not go as far as the one provided by Art. 13 et seq. GDPR.
- The new SCCs require *all* importers - including processors and their sub-processors - to provide information on their website or directly to the data subjects with a contact address for

complaints (and oblige them to deal with these in an expeditious manner) (Clause 11). This goes beyond the GDPR, where only the controller is obliged to inform the data subjects.

Furthermore, the new SCCs provide for certain notification obligations vis-à-vis the data subjects. These are, on the one hand, an obligation to report breaches of data security if they entail a high risk of adverse effects for the data subject (e.g. Module 1, Clause 8.5(f)) and, on the other hand, an obligation to report if a foreign authority accesses or attempts to access the personal data of the data subject (Clause 15.1).

36. Where do the new SCCs expose us to data subjects and organisations like NOYB?

All provisions of the new SCCs are also directly enforceable by the data subjects, unless they are listed in the relatively short catalogue of exceptions in Clause 3.

The provisions in question thus constitute a contract for the benefit of third parties, which is enforceable under Swiss law (even if the CH DPA does itself not require such third party beneficiary rights under Art. 6(2)(a) CH DPA). However, this is not the case everywhere. Irish law, for example, does not allow claims in favour of third parties (Ireland has meanwhile clarified in its law that third party beneficiary rights are enforceable in the context of the SCCs).

For the parties to the SCCs, the claims in favour of data subjects mean two things:

- All provisions that prescribe conduct in favour of the data subject (e.g. providing information, taking a certain protective measure) can be enforced by the data subject in court. Under Swiss law, such claims are enforceable as specific performance. In other legal systems, sometimes only damages can be claimed. It is questionable whether the choice of such contractual law is permissible, as the SCCs clearly aim at specific performance. The authors have overlooked this aspect, though, as they don't require that the choice of law has to enable claims for specific performance.
- Any breach of the SCCs (with the exception of the provisions listed in Clause 3) that causes damage to the data subject gives rise to unlimited contractual liability towards that person. This includes breaches of conduct (i.e. provisions requiring the exporter, importer or all parties to act in a certain way) as well as breaches of warranties (e.g. Clause 14(a)). This claim for damages is only directed against the controller. However, joint and several liability already exists (Clause 12(c)). Under Swiss law, the party liable under the SCC must be at fault, but that would be presumed.

The previous SCCs already provided that data subjects could assert claims. In practice, however, this played virtually no role, as proceeding would entail considerable litigation risks. The civil procedural facilitations, which are partly intended for data protection litigation, do not apply here, as it is ultimately a matter of normal contractual claims.

It should be noted, however, that data subjects can also entrust a non-profit organisation such as NOYB with the enforcement of their claims. For them, the new SCCs thus open up a new, broad playing field.

37. How does the enforcement of the new SCCs work? What happens if we do not comply with the requirements of the SCCs?

Enforcement takes place on three levels:

- By the contracting parties: The SCCs create contractual obligations for the parties. If one party does not comply with its obligation, the other party can enforce it by taking legal action in the form of a claim for damages or - where the applicable law permits - in the form of actual performance. This is the weakest form of enforcement. It is true that the exporter in particular will have an interest in enforcement because it can only rely on it for the transfer of personal data to non-whitelisted third countries if it not only concludes it but also enforces it against the importer. Nevertheless, past experience shows that exporters hardly ever assert claims under SCCs, even though the instrument has been in existence for 20 years now. In addition, some obligations are formulated in such a way that enforcement by one party against the other is not straightforward, for example because they are imposed jointly on the parties (e.g. Module 4, Clause 8.2(a) or Clause 14(a)). This is poor drafting.

  If there is a material or persistent breach of the SCCs, the exporter naturally has the right to terminate (Clause 16(c)). What is less self-evident is that it will need to check very carefully whether it actually wants to terminate. If it does so, it must notify the supervisory authority and may expose itself (Clause 16(c)). However, it is questionable whether the violation of this obligation can be sanctioned at all. In any case, it does not seem to have been thought through completely. The termination clause is also defective in other respects (question 42).

- By the supervisory authority: The SCCs provide in some places for the obligation to do something for the benefit of the supervisory authority (e.g. to report a data breach in Module 1, Clause 8.5(b) or to provide the documentation of its own processing activities in Module 1, Clause 8.9(b)). However, the SCCs do not provide the supervisory authority with a contractual right to en-

force these obligations in its favour in court, although this would have been contractually possible. Is the intention: The only third party that Clause 3 provides with a right to claim is the data subject; from this it must be concluded, at least in the case of Swiss law, that the supervisory authority has no such (contractual) claims, which is ultimately a missed opportunity for enforcement.

Instead, Clause 13(b) provides that the importer (which by its nature is *not* subject to the GDPR) voluntarily "submits" to the jurisdiction of the supervisory authority designated by the parties and agrees to cooperate with it. However, we have considerable doubts about the legality of this construction. Ultimately, this can only be answered according to the law of the respective supervisory authority, but in Switzerland such a "contractual" jurisdiction of the authority would probably be ineffective, because the jurisdiction of an authority arises solely according to the law applicable to it and not because one party has committed towards another party in a private contract to submit itself to such jurisdiction. Also under the GDPR, the competence of a supervisory authority arises exclusively from Art. 50(1) GDPR and thus, according to the principle of territoriality. It also presupposes the applicability of the GDPR according to Art. 3 GDPR. Neither of these will be fulfilled in some of the cases relevant here - not even according to the liberal requirements of Recital 122 of the GDPR.[15]

The situation is different for the exporter who, depending on the case scenario, is subject to the jurisdiction of a supervisory authority (but not necessarily the one chosen in Clause 13) independently of the SCCs. In this way, the SCCs can at least be indirectly enforced against the importer: If the exporter does not enforce the SCCs against the importer or does not comply with them itself, it must expect that the supervisory authority will sanction it for undertaking a data transfer in violation of Art. 46 DPA. This provision does not explicitly require compliance with and enforcement of the SCCs, but if there is no implicit obligation to comply and enforce the SCC, they would be pointless. Non-compliance with the SCCs therefore exposes the exporter in particular to a risk of sanctions.

Swiss law applies similarly, but with certain differences:

- If a party does not comply with the SCCs, it must first be examined whether the required level of data protection is lacking as a result. This is not necessarily the case. If, for example, an obligation is breached that goes beyond the GDPR or the CH DPA (e.g. in the area of documentation

15 Accordingly, there is already a competence for controllers or processors when they carry out processing activities that are "targeted" at data subjects in the territory of the authority.

obligations), then it cannot reasonably be argued that data protection has been breached. Even the future Art. 16(2) revised CH DPA only requires that a "suitable" level of data protection is ensured - but not identical and certainly not better data protection than would exist under the CH DPA in Switzerland (some provisions of the SCCs go beyond this, however). If there is a lack of adequate data protection because the importer does not comply with his obligations, the FDPIC can intervene and, for example, prohibit further transfer of the data (Art. 51 para. 2 revised CH DPA). What it cannot do, because Art. 51 revised CH DPA does not provide for this, is to demand that the exporter contractually enforce the SCCs. If the FDPIC cannot prosecute the importer itself under supervisory law, it has no means of action against it. The "contractual" submission to the FDPIC's jurisdiction discussed above for the GDPR is unlikely to be enforceable in Switzerland.

- In parallel, the penalty provision of Art. 61(a) revised CH DPA can apply if the exporter continues to disclose personal data abroad even though it knows that the importer does not ensure appropriate data protection despite the contract because it does not or cannot comply with the contract. The breach of contract itself, however, cannot be fined; the wording of Art. 61(a) revised CH DPA is too restrictive for this. Under current law, no fine is possible for a violation of Art. 6(2) CH DPA on the basis of the CH DPA. The importer cannot be fined, as only the disclosure of personal data is punishable - not its receipt or use in breach of contract or data protection.

  Pro memoria: A foreign data protection supervisory authority cannot compulsorily enforce orders or fines in Switzerland because doing so would make itself and the cooperating Swiss party liable to prosecution (Art. 271 Swiss Criminal Code).

- By the data subject or a representative: c.f. question 36.

In practice, the enforcement of or compliance with the SCCs has played a rather subordinate role so far. With "Schrems II", this has changed with regard to the protective measures to be taken for your data transfer: Here, certain supervisory authorities in the EEA have begun to ask exporters questions. It can be assumed that such supervisory activity will increase.[16]

[16] Cf. https://www.lda.bayern.de/de/thema_schrems2_pruefung.html.

38. What about liability under the new SCCs?

Under the new SCCs, the parties are not only liable to the data subjects for breaches of the SCCs, but also to each other (Clause 12).

The previous SCCs provided for mandatory liability in favour of data subjects (which was barely relevant in practice so far), but mutual liability of the contracting parties was optional. The clause proposed by the European Commission in the previous SCCs was hardly ever used in practice.

Now, the mutual liability of the contracting parties is a mandatory provision that may not be amended or restricted, either directly or indirectly. At least that is our understanding. The SCCs thus go beyond the requirements of the GDPR, which even for data processing arrangements does not stipulate unlimited liability for either the processor or the controller. In practice, unlimited liability is rarely agreed upon; however, a so-called "super cap" is often seen, i.e. a maximum liability amount that is higher than the rest of the contract - insofar as the liability can be limited or waived under the applicable contract law.

It is still possible for a client and a provider to agree on a limitation of liability in a service contract, but to the extent that the SCCs apply and a provision of the service contract conflicts with it, the SCCs prevail (Clause 5) and must do so in order for the SCCs as such to remain valid (Clause 2(a)). Thus, the question arises whether a limitation of liability in the service contract is in conflict with the liability provision in the SCCs. If this is the case, the former does not apply to the extent that a liability claim can be based on Clause 12. It even provides that an importer cannot exculpate itself if it is not responsible for the damage but rather his processor or sub-processor. It is thus stricter than Art. 84(3) GDPR, according to which a controller can exempt itself from liability if it proves that it is not responsible in any respect for the circumstance that caused the damage.

In practice, various questions arise which at the same time offer approaches as to how the parties to SCCs can possibly limit their mutual liability risk:

- Does Clause 12(a) actually conflict with a contractual limitation of liability? The wording leaves room for manoeuvre depending on the language version of the SCCs. In the English version, Clause 12(a) states that a party is liable to the other party "for any damages". The German version is less absolute. It only states that each party is liable to the other parties "für Schäden" it causes which translates as "for damages". This wording leaves room for argumentation, according to which Clause 12(a) merely states the principle of liability, but leaves room for further clauses limiting liability. In fact, many commercial contracts contain wording that on the one hand states that parties are liable to

each other for damages, but in a further clause excludes or limits this liability in certain cases. That said, a limitation of liability in a service contract would not be inconsistent with Clause 12(a). After all, there is a risk that a data protection authority would take the position that Clause 12(a) should be interpreted as a conclusive provision because it creates a strong incentive to comply with the SCCs, which in turn is in the spirit of the GDPR and therefore decisive for the interpretation (Clause 4(b)). Clause 12(a) would otherwise be weakened, which would contradict Clause 2(a).

- Another relevant question will be *what* damages a party to the SCCs can claim under Clause 12(a). This applies in particular to data processing arrangements, where the data processing is a contractual service of one party (the processor), which it is typically never prepared to offer without extensive limitations and exclusions of liability.

  The answer is ultimately a question of the applicable contract law, not the GDPR. One starting point is the purpose of the contract which results from Clause 1(a), namely compliance with the GDPR when processing personal data. From this, the argument can be made that the liability clause only targets damages from which the GDPR also aims to protect: Anyone who has to take its online shop out of operation for three days due to a data breach and thus suffers a loss of profit has no such damage. The situation would be different if, due to inadequate data security on the part of a provider, the client incurs expenses to restore lost personal data - this is the expense to restore the position that would have existed if there had been proper processing of personal data.

  Swiss law allows for such a consideration. It is based on the so-called protective purpose theory, which an increasing number of Swiss authors also want to apply to claims under Art. 97 of the Code of Obligations (CO), which is at issue here, within the framework of the consideration of adequacy. In recent decisions, the Federal Supreme Court has also included the purpose of the specific liability norm in question in the assessment of adequacy.[17] In the case of damage in connection with the SCCs, it could therefore be argued that the protective purpose theory applies here in full (or at least in part) and that Clause 12(a) therefore only intends and permits damages for "data protection damage", i.e. for all other damages the liability provision in the parties' main contract would apply. In order to avoid

[17] DFC 123 III 110 consid. 3a p. 112 et seq., Decision 4C.422/2004 of September 12, 2005 consid. 5.2.2.1, Decision 4C.103/2005 of June 1, 2005 consid. 5.1 and Decision 4A_87/2019 of September 2, 2019 consid. 4.3.1 et seqq.

contradictions, it could be stated there that the limitation of liability in the main contract does not apply to "data protection damages" which can be claimed under Clause 12(a) of the SCCs. What exactly such data protection damages are is another question. They are unlikely to include lost profits and the like.

We expect that there will still be some discussion on the scope of the liability clause and the possibility of avoiding extensive liability.

For claims for damages by data subjects, see question 36.

39. What is the legal significance of the warranties given?

This question is decided according to the applicable contract law.

Under Swiss law, the breach of one of the (few) warranties in the SCCs leads to a claim for damages for breach of contract. The warranty case must exist at the time the contract enters into force. In the case of Clause 14(a), the parties must therefore already have reason to believe at the time of the conclusion of the contract that the importer's domestic law will prevent its compliance with the SCCs. If this is the case, a data subject may, if the conditions are met, seek compensation for the damage caused by an event which the parties (or one of the parties) had reason to believe might occur. If they did not have to expect it because it was so unlikely, they are not liable in any case under Swiss law.

40. What do we have to do to meet the requirements of Schrems II? Are the new SCCs sufficient?

No, the new SCCs are not sufficient. The parties must also (i) ensure that they can comply with the SCCs regardless of the importer's domestic law and (ii) document their assessment in this regard. In other words, a so-called *Transfer Impact Assessment* (**TIA**) must be carried out and data may only be transferred if this TIA is satisfactory. For information on how to conduct the TIA, see question 41.

The focus of a TIA is on whether the importer (and other recipients in the chain) can be compelled under its law by a local authority to hand over personal data *and* whether such lawful access fails to meet standards of EU law. This last subsentence is important: If a US court orders a US provider to hand over personal data of its European client in the context of civil or criminal proceedings, this is in principle not in conflict with EU law. The US CLOUD Act is also not in conflict with European law - on the contrary, it implements Art. 18 of the Council of Europe Cybercrime Convention. Such access is also always possible at any time within Europe.

That said, an obligation to surrender data, which is *not* subject to judicial review, is not compatible with the standards of EU law. This was the only issue in Schrems II.[18]

In the context of a TIA, it must therefore be examined whether the importer can be forced to hand over personal data without being able to defend itself or the data subject in court.

Initially, there was disagreement about which outcome of a TIA would permit the transfer of personal data based on the SCCs to take place. In an initial opinion, various EU data protection authorities and the European Data Protection Board (**EDPB**) took the view that the risk of such access without a guarantee of legal recourse must be zero. This was widely criticised. In the meantime, the EDPB has revised its position and accepts a residual risk in version 2.0 of its recommendation 01/2020 of June 18, 2021[19]. Addressing exporters, the EDPB states: You "may" transfer personal data to a non-whitelisted third country even without additional measures (besides the SCCs) if "you consider and are able to demonstrate and document that you have no reason to believe that relevant and problematic legislation will be interpreted and/or applied in practice so as to cover your transferred data and the importer".[20]

According to our practical experience, a reasonable TIA, at least with regard to the USA, concludes in almost all cases that there is no relevant risk of access by authorities without a guarantee of legal recourse and therefore a transfer of personal data under the SCCs to a non-whitelisted third country must be permissible. Nevertheless, the TIA must be carried out and documented according to the EDPB and the SCC.

Many experts (correctly) consider the effort that the EU data protection authorities require to expend on this to be disproportionate. With their first extreme, impractical and above all seemingly panicked reactions to the ECJ ruling on "Schrems II", the EDPB and many individual authorities have positioned themselves in a corner from which they will now find it difficult to escape without losing face. In order to justify the position that data transfers to the USA should now be possible again even without full encryption, because the danger of access by the authorities without a guarantee of legal recourse is not as great as previously feared in most cases, the requirements for a supporting TIA are now being cranked up accordingly. Even for standard situations,

---

18 Specifically, it concerned two provisions of US law in which US intelligence services are allowed to access European data under certain, special constellations, without this being subject to a legal recourse guarantee. The US COUD Act was not the subject of Schrems II. See also https://www.vischer.com/know-how/blog/schrems-ii-was-er-fuer-unternehmen-in-der-schweiz-bedeutet-38295/.

19 https://edpb.europa.eu/news/news/2021/edpb-adopts-final-version-recommendations-supplementary-measures-letter-eu_en.

20 EDSA, Recommendation 01/2020, Executive Summary and para. 43.3.

the EDPB requires a "detailed" report[21] written for the specific individual case, with evidence from publicly accessible, documented sources[22]. We expect this requirement in many cases not be follow-up in practice and slowly erode over the next years.

Some will probably think that it would be more beneficial for the data subjects if the resources to be spent on this by the exporter were invested in data security audits instead. For example, in our practical experience, a data security *audit* would be much more important and effective for the protection of data subjects than a TIA, since today personal data are much under threat from a lack of data security than from access by foreign authorities without a guarantee of legal recourse. However, such audits rarely occur.

In our opinion, it is acceptable to carry out a transfer if it is highly unlikely that there will be any foreign authority access without a guarantee of legal recourse even if no detailed and formalized TIA has been performed. In our opinion, this is permissible without issue under Swiss law. The same must apply to the GDPR, even if, as mentioned, conflicts with EU data protection authorities are conceivable. In practice, however, we have had good experiences with this position if it can be shown to a data protection authority that, on the one hand, an exporter has dealt with the issue in appropriate detail and can justify its position under foreign law as well and, on the other hand, has also taken corresponding measures to reduce the risk of such authority access. For this purpose, we have developed a (freely available) statistical method to comprehensibly and concretely calculate the probability of foreign authority access in the sense of a predictive judgement for the purposes of a risk decision.[23] This has proven itself in practice and is now regularly used in Switzerland for more sensitive cases, such as determining the probability of data protected under professional secrecy being exposed to foreign lawful access. In our view, what is suitable for banking secrecy must be suitable also for data protection purposes.

We also expect the major cloud providers to start providing their clients with information and templates for TIAs to standardise this process as much as possible.

The new SCCs also follow the risk-based approach. The parties do not have to warrant that no foreign authority access can occur without a

---

21 EDSA, Recommendation 01/2020, footnote 54 "Reports you will establish will have to include comprehensive information on the legal assessment of the legislation and practices, and of their application to the specific transfers, the internal procedure to produce the assessment (including information on actors involved in the assessment-e.g. law firms, consultants, or internal departments-) and dates of the checks. Reports should be endorsed by the legal representative of the exporter."

22 EDSA, Recommendation 01/2020, Annex 3.

23 https://www.rosenthal.ch/downloads/Rosenthal_Cloud_Lawful_Access_Risk_Assessment.xlsx and the scientific contribution to it at https://www.rosenthal.ch/downloads/Rosenthal-CloudLawfulAccess.pdf.

legal recourse guarantee, but only that they have "no reason to believe" that such access will occur in their case. This means that we are moving - to use a term from Swiss law - in the area of contingent intent: Success is considered possible and, although it is not sought, it is ultimately taken into account, i.e. accepted. "Conscious negligence" is not sufficient: This would be the case if the exporter considers the access to be possible but trusts ("believes") that it will not happen. Even according to the doctrine of contingent intent, this is of course not possible if the probability of occurrence is arbitrarily high - if the probability of the success exceeds a certain level it is assumed that the data subject must have expected success.

In practice, these considerations will be superfluous, because in the vast majority of data transfers in everyday business, the probability of occurrence will be so low that not even an accusation of negligence could be justified. If the standard required by the new SCCs is taken as the measure of all things, a transfer would therefore not be problematic and the warranty of Clause 14(a) would not be violated.

All of this also applies to transfers from Switzerland. On June 18, 2021, the FDPIC published a guide for checking the admissibility of data transfers with a foreign connection in accordance with Art. 6 para. 2 let. a DPA.[24] This also requires an examination of the legal situation in the target country, taking into account the applicable legal provisions in the target country, the practice of the administrative and judicial authorities and case law. The original version of the instructions still contained the sentence: "Subjective factors such as the probability of access cannot normally be taken into account." This was subsequently (and rightfully) deleted, because it is simply wrong: The probability of access is not a subjective factor, but ultimately the result of the analysis. For Switzerland the same applies as for the EEA: The probability of foreign lawful access without legal recourse does not have to be zero. Legal opinions also never provide certainty; their statements are usually much more imprecise and subject to more noise, bias and reservations than the expert judgement based on the statistical method already mentioned. It is true, however, that it cannot simply depend on a "feeling" as to whether a foreign authority access without a guarantee of legal recourse will occur.

The new SCCs not only regulate under which conditions (in the view of the European Commission) transfers may be made, but also what is to be done in the event of a threat of access by authorities. This is not a contradiction of the warranty that the parties do not expect access without a legal recourse guarantee, because the Clause 15 in question covers all forms of surrender orders or access by foreign authorities, including those subject to judicial review. For these cases, the SCCs

---

24 https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/handel-und-wirtschaft/uebermittlung-ins-ausland.html#-2053327153 (in German).

now provide on the one hand in Clause 15.2 a "defend your data" (i.e. a clause imposing an obligation to defend the data by legal means and action against the release order or access) and on the other hand in Clause 15.1 a reporting obligation.

This reporting obligation is a serious one, as it not only requires the exporter to be informed, but also the data subjects (Clause 15.1(a)). Hence, if a bank outsources its data to the cloud of a European provider and this provider involves a sub-processor in the USA through which a US authority wants to access the bank's client data, then according to the wording of the SCCs the sub-processor in the USA would have to write to the bank's clients and the bank would ultimately have to provide it with the necessary information to complete this task. This is not only impractical, but also contradicts data protection principles, since in this case the sub-processor would have to be given even more personal data than it already has, under the pretext of data protection. In such cases, it is advisable for the parties to delegate the notification of the data subject to the controller, which in our opinion must be permissible (Clause 4(c): The SCCs are to be interpreted in compliance with data protection).

41. How is a Transfer Impact Assessment (TIA) done under the new SCCs?

Transfer Impact Assessments are regulated in Clause 14(b), at least partially. A TIA is required if personal data is to be transferred to a non-whitelisted third country on the basis of the SCCs (see question 40).

A TIA answers the question of what possible negative effects the transfer of the personal data to the destination country may reasonably have for the data subjects, and how probable they are. These can be any kind of negative effects. For example, if there is a state of emergency in the destination country, this may have an impact on data security or otherwise on the reliability of the processing of the data in accordance with data protection law. Of course, before transferring personal data to a third party, an exporter must consider whether the personal data (and thus also the data subjects) are at risk of any harm.

In the context of Clause 14(b), however, a TIA is construed much more narrowly. For the purposes of Clause 14, a TIA must answer the question of how probably it is that, as a result of the transfer of the data to the destination country, the authorities there could access or demand the release of the personal data without this process being subject to judicial review. This refers, for example, to intelligence service "dragnet searches", with which all transmissions of a provider (e.g. a social media platform or an email provider) are searched for certain keywords for the purpose of fighting terrorism, without the necessity of a court order or the possibility of an appeal against the

processing. Such access under US law was the subject of the "Schrems II" ruling.

Clause 14(b) states that all the circumstances of the individual case must be considered, including the nature of the data, the data processing and the data processor, the previous experience with access by authorities in the scenario in question and the measures taken to protect against access by authorities. In other words, this means that a risk assessment must be carried out and it is not necessary - at least in the view of the European Commission - that access by a foreign authority is completely prevented in technical terms, e.g. by means of full encryption. According to Clause 14(b), such technical measures are only one of several factors to be considered in the TIA. Data protection authorities have made clear, though, that it is not sufficient to rely on the data at issue not being "interesting" to the foreign authorities. An analysis of the foreign law and the way it is applied is necessary, if technical measures can't prevent unwanted lawful access.

By law, it is the exporter who must carry out the TIA. However, if the SCCs are signed, the importer is at least contractually obliged to provide all the information required for the TIA to the best of its knowledge and belief and must explicitly warrant having done so (Clause 14(c)). Thus, if a TIA turns out to be insufficient or incomplete and the exporter suffers a loss as a result (e.g. because it cannot perform his contract as planned following the intervention of a data protection authority), the importer risks compensation claims from the exporter if it has not informed it or not correctly or not completely informed it, about the access risks under his domestic law. The same applies if it does not inform it about amendments to his domestic law (including court practice) (Clause 14(e)). This applies to the entire chain of subcontracted processors.

Service providers in non-whitelisted third countries are thus advised to inform their clients in Europe about access risks and access cases on their own initiative, so that they can carry out their TIA and adapt it if necessary. Customers in Europe are in turn recommended to ask their service providers for this information. The SCCs do not contain a provision on the bearing of costs. However, we assume that standard TIAs will emerge for certain standard use cases, with which the parties can fulfil their obligations and no longer have to obtain corresponding legal opinions for each data transmission. However, the EDPB still assumes the latter model in its recommendation 01/2020[25]. Even for standard situations, it requires a "detailed" report[26] written for the

---

25 https://edpb.europa.eu/news/news/2021/edpb-adopts-final-version-recommendations-supplementary-measures-letter-eu_en.

26 EDSA, Recommendation 01/2020, footnote 54: "Reports you will establish will have to include comprehensive information on the legal assessment of the legislation and practices, and of their application to the specific transfers, the internal procedure to produce the assessment

specific individual case. This report must be based on publicly available sources and show the application of the provisions of foreign law that conflict with a prohibited access by the authorities for the sector concerned (for classification, c.f. also question 40). At least the EDPB accepts that not just the mere letter of law is relevant, but also the concrete application of the provisions in practice.

Also illustrative for the documentation of a TIA are the questionnaires[27] developed by the Bavarian data protection authority, the BayLDA, for various applications. The form from NOYB, with which US importers can be asked for information about their own access risk[28], can also be helpful in relation to the USA; however, it is unlikely to meet the requirements of the EDPB, as it does not contain any evidence and does not go into enough depth in other respects - which is paradoxical insofar as it was in fact NOYB that triggered "Schrems II" in the first place. It is to be hoped that the emotions will calm down a bit in this regard as well and that the requirements for a TIA for manifestly harmless standard situations (such as the transmission of HR data to a parent company in the USA) will be reduced to a reasonable level, especially since it can be argued with good reason that the feared US intelligence access in such cases is already ruled out due to the fact that in such cases data is transmitted to US persons. Alan Charles Raul's essay is interesting in this regard, showing why of all things the conclusion of the SCCs also legally protects the transmitted data from access under Section 702 FISA and EO 12.333.[29]

Finally, we have developed a (freely available) statistic method of how to calculate the probability of a foreign authority access in the sense of a predictive judgement for the purpose of a risk decision in a comprehensible and concrete way. The method has been implemented in the form of an Excel.[30] It already contains an exemplary assessment of the risk of access from the USA when using a Swiss or European cloud as offered by companies such as Microsoft. Although the method was originally developed for the purposes of professional secrecy protection, it also works for the purposes of Clause 14(b) and has proven itself to work in practice. It covers not only access by public authorities without legal right to recourse but also other access by foreign authorities and courts. If one decides to meet the requirements of the EDPB, it may have to be supported with a legal opinion.

(including information on actors involved in the assessment-e.g. law firms, consultants, or internal departments-) and dates of the checks. Reports should be endorsed by the legal representative of the exporter."

27 https://www.lda.bayern.de/de/thema_schrems2_pruefung.html.

28 https://noyb.eu/files/CJEU/EU-US_form_v3_nc.pdf.

29 See Alan Charles Raul (Sidley), Schrems II Concerns Regarding U.S. National Security Surveillance Do Not Apply to Most Companies Transferring Personal Data to the U.S. Under Standard Contractual Clauses (https://bit.ly/3cWsyXB).

30 https://www.rosenthal.ch/downloads/Rosenthal_Cloud_Lawful_Access_Risk_Assessment.xlsx and the scientific contribution to it at https://www.rosenthal.ch/downloads/Rosenthal-CloudLawfulAccess.pdf.

42. What technical deficiencies do we need to look out for in the new SCCs?

Some points of the new SCCs have not been thoroughly thought through or well drafted. Here is a selection of shortcomings and corresponding workarounds:

- Clause 7: There is no provision on how to ensure the consent of the existing parties to the entry of a new party into the contract. Solution: Omit clause 7 and regulate separately.
- Module 3, Clause 8.1: It is wrongly assumed that in a chain of several processors at most the first link is located in the EEA or a whitelisted third country. Solution: Ignore.
- Module 2, Clause 8.8: It is not clear who is responsible for ensuring compliance with the requirements for the onward transfer of data. Solution: The processor obliges the controller to only instruct the onward transfer if the requirements according to Clause 8.8 are fulfilled.
- Onward transfer provisions: There is no reservation regarding the publication of personal data, insofar a publication is permissible. In principle, a publication is not considered to be a transfer of personal data to a third country. Solution: Ignore the deficiency.
- Clause 9: Although it is provided that a sub-processor can be rejected, there is no regulation as to what happens in this case. An interpretation of the clause according to its purpose will result in the understanding that such a sub-processor cannot be used. Solution: Regulate the consequences separately, e.g. by means of a right of termination, if the notice period is sufficiently long.
- Clause 9: There are no provisions on sub-processors in the case that the processor is in the EEA but the controller is not. The use of sub-processors is also conceivable in these cases, and their use would basically have to be regulated under Article 28 GDPR. Solution: Regulate separately.
- A module is missing for the case that the sub-processor is subject to the GDPR, but his processor is in a non-whitelisted third country. Solution: Use module 4 (if the controller is not subject to the GDPR) or module 3 (in the other cases).
- Clause 9(b): A sub-processor in a non-whitelisted third country is not required to enter into the SCC with its own sub-processor in a non-whitelisted third country. Notably, the processor is liable for the sub-processor only to the extent that it does not comply with the contract it has concluded with the sub-processor. Even more, the SCCs do not provide that the sub-processor is generally responsible for the conduct of its own sub-processor. This flaw results in a loophole. Solution: Apply the SCC also vis-à-vis the subprocessor.

- Clause 13: There is no provision for the situation where a representative has to be appointed according to Art. 27 GDPR, but it has not been done. Solution: Use the third option.
- Clause 13: The "contractual" submission to the jurisdiction of the chosen EEA supervisory authority over the importer is likely not enforceable, because the jurisdiction of the EEA supervisory authority arises conclusively from the GDPR, which does not provide for such a competence for a foreign importer, which by nature is not subject to the GDPR. Solution: Ignore the deficiency.
- Clause 15.1: The obligation of every importer to inform the data subject directly in the event of foreign authority access or attempted access, will in many cases not protect their data protection rights, but rather violate them, because the importer in question must be provided with even more information about the data subjects. Solution: The notification of the data subject should be delegated to the controller.
- Clause 16: Sub-clause (c) states that the exporter may terminate the "contract" in the event of a breach of the SCCs "insofar as" it relates to the processing of personal data. Firstly, it is not clear what "contract" refers to (probably not only to the SCCs, but to the main contract that the SCCs serve, but see below), and secondly, such a provision leads to uncontrollable results, as it only (but still) allows the terminating party to partially terminate the main contract. Solution: This termination option should be caught by the main contract. Moreover, the clause does not specify in any way how the termination has to be effected and within which time limits. Notably: If the importer indicates that it can no longer comply with the SCCs, termination is only possible after a deadline has been set (cf. Clause 16(c)(i)).

  The references to the main contract are problematic because this main contract does not necessarily exist between the parties that concluded the SCCs. In the previous standard contract with Microsoft, for example, European clients conclude their main contract with Microsoft's Irish company, but the SCCs with Microsoft Corp. Since there are no contracts at the expense of third parties, the right to terminate the main contract stipulated in the SCCs is meaningless. The obvious solution in such cases is not to conclude the SCCs with a sub-processor (question 30), but this has to be balanced against the fact that such a direct conclusion of the SCCs contract can of course also bring advantages for the client, as it gives rise to additional claims.

  There is another shortcoming in this provision: If the exporter terminates on the basis of Clause 16(c) due to non-compliance with the SCCs, it is obliged under the same clause to report this

to the supervisory authority. Even if it is not clear how this provision is to be enforced, this obligation is particularly likely to deter the exporter from giving notice - which is certainly not the intention.

- Clause 18: The jurisdiction refers to the country, not the city or the judicial district. This means that jurisdiction is not clear or at least has to be clarified according to the domestic jurisdiction rules. Solution: Specify the place, not just the country.

A fundamental flaw not in the SCC themselves, but in their issuing by the European Commission is the restriction to transfers to importers who are not themselves subject to the GDPR, which makes no sense (see question 7). However, we believe that the last word has not yet been spoken on this point. Solution: Ignore.

43. **When we work with lawyers in the USA for an official or court case what part of the SCCs do we use? Does this still work?**

Yes, the new SCCs can be used here and actually improve the situation. However, it is important to distinguish between two situations:

- The disclosure of personal data to one's own lawyers and group companies abroad for the purpose of conducting foreign official or legal proceedings. Here the SCCs will continue to be used.
- The disclosure of personal data to the opposing party (namely in the case of *pre-trial discovery*) or foreign authorities or courts. Here, the SCCs do not come into play, but instead the exception of Art. 49(1)(e) GDPR applies, whereby it must be ensured that the disclosed data are only used for the purposes of the relevant authority or court proceedings in question (e.g. with a *Protective Order*).

If the SCCs are used, both Module 1 (Controller-Controller) and Module 2 (Controller-Processor) may be applicable, depending on the specific case scenario. In the past, the Controller-Processor SCCs were preferred because the Controller-Controller SCCs effectively prevented the disclosure of personal data in the foreign authority or court proceedings due to their restrictive wording: The data could be disclosed to US attorneys for US proceedings, but they were not allowed to use it in the trial. The Controller-Processor SCCs did not regulate disclosure in this way; it was a matter of the controller's instruction.

The new SCCs elegantly solve the problem by allowing disclosure by the importer in both Module 1 (Clause 8.7(iv)) and Module 2 (Clause 8.8(iii)) if this is necessary for the assertion, exercise or defence of legal claims in supervisory, regulatory or judicial proceedings abroad.

This solves the problem. Therefore, with one's own lawyers abroad, the new SCCs can also be agreed in Module 1.

44. Do we still need a data processing agreement if we use the new SCCs?

No, not from a purely legal point of view, because in contrast to the previous SCCs, the new SCCs fulfil all the requirements of Art. 28(3) of the GDPR according to the European Commission. They are considered to be approved standard clauses for data processing arrangements within the meaning of Art. 28(7) GDPR (Clause 2(a)).

In practice, there will still be a need for further agreements in many cases, namely on the way instructions are issued, on the bearing of costs and on filling the gaps in the regulations contained in the SCCs (e.g. on the consequences of refusing a sub-processor). This can be implemented, for example, in a service provider contract in such a way that the main contract contains a base contract under data protection law with the necessary specifications and supplements, which then either declares the necessary Modules and options of the full SCCs to be part of the contract and contains the individual details in an annex or refers to an annex which contains a completed variant of the SCCs already reduced to what is specifically applicable to that particular case.

The situation is different where a data processing agreement is to be concluded between two parties who are both either in the EEA or a whitelisted third country. Here, the SCCs are not required per se and it must be expected that the authorisation of the SCCs as a data processing agreement within the meaning of Art. 28(7) GDPR does not apply to this case because the European Commission has not provided for the use of the SCCs in this situation. However, this does not mean that SCCs *may* not be used in these cases. In our view, this is permissible (question 8). Accordingly, it must be possible to use the SCCs as a data processing agreement also between a controller and a processor (or between two processors) who are *both* in the EEA or a whitelisted third country. Formally speaking, the wording of the SCCs does not quite correspond to the requirements of Art. 28(3),[31] but the deviations are within the usual background noise in practice.

In practice, most parties will not be interested in using the SCCs voluntarily, as they are quite far reaching. It is therefore not to be expected that the SCCs will be used more often as a template for data processing agreements for commissioned processing in the EEA and in

---

[31] The duty of support of the processor does not refer to the obligations of Art. 32 to 36 GDPR (Art. 28(3)(f) GDPR) and can therefore only be justified indirectly with reference to the preparation of data protection impact assessments. The equivalent to Art. 28(3)(a) and (g) GDPR is also formulated somewhat more liberally in the SCCs, in that the SCCs provide for a reservation in favour of the processor's domestic law, whereas the GDPR only allows such a reservation for the law of the EEA and its Member States.

white-listed third countries. This is all the more true for data processing arrangements under Swiss law, where the requirements are even lower. In addition, the European Commission has presented its own standard contractual clauses (i.e. the SCCs-DPA) for this case, which, however, are not very attractive for the same reasons, especially since they may not be changed if they are to be used under Art. 28(7) GDPR.

In the case of IGDTAs, however, the use of the SCCs as a data processing agreement can make sense. This is because an IGDTA regulates not only the transfer of personal data to non-whitelisted third countries, but also commissioned processing within the EEA and in transactions with third countries. In such a scenario, it sometimes makes little sense for these cases to provide for a different regulation in the IGDTA than that which applies under the SCCs. On the contrary, it may even be appropriate to provide for the same rules for the entire group when internal processing occurs - whether in a country with or without adequate data protection.

Nevertheless, we expect that there will always be IGDTAs in which the new SCCs-DPA will also be used, for example in IGDTAs in a purely European context or where the authors want to "play it safe", even if this is at the expense of the readability and unity of the contracts.

However, many people will consider the SCCs-DPA more cumbersome and less attractive than the individual data processing agreements that have become established in practice. Moreover, they have similar weaknesses to the SCCs (but are not identical to them):

- They do not regulate the consequences of an objection to the appointment of a new sub-processor (Clause 7.7). The new SCCs also have this technical deficiency.
- They contain an unnecessarily complicated regulation regarding the notification of data security breaches by distinguishing between breaches on the part of the controller (in which cases the controller must be supported by the processor) and those on the part of the processor (Clause 9). It remains unclear when exactly each of the provisions applies.
- Like the SCCs, they go beyond the GDPR (e.g. information about incorrect data, disclosure of documents to data protection authorities, scope of TOMS).
- They do not contain any provisions on the bearing of costs.

However, individual parties may always bring up the SCCs-DPA in contract negotiations or refer to the model regulation of the SCCs-DPA when negotiating individual data protection agreements, e.g. if there are differences regarding the deadline for reporting a data protection breach (which neither the SCCs nor the SCCs-DPA recognise).

45. What specific actions should we now take as a company?

For a European company that is not itself primarily active as a processor, a typical approach is as follows:

- The existing IGTDA, i.e. the contractual regulation of intra-group data exchange (see question 46), will be adapted by 27 September 2021 - at least to the extent that group data also flow to non-whitelisted third countries. Note: If the IGDTA also regulates data flows from third countries with their own data protection laws, these must also be observed. For Switzerland see question 9**,** for the UK see para 21.
- The privacy statements must be adapted accordingly. As is well known, they must explicitly mention the safeguards under Art. 46 GDPR and indicate where it is available or where a copy can be obtained (Art. 13(1)(f) GDPR, Art. 14(1)(f) GDPR; Art. 19(4) revised CH DPA).
- An overview is provided of other cases in which personal data are communicated to non-whitelisted third countries. Optimally, these data transfers are to be taken from the list of processing activities.
- The entries in this list are divided into three groups:
  - The first group comprises those cases in which client contracts are affected. These cases should be prioritised: If the client is located in a non-whitelisted third country, it may not be very easy for the company to persuade it to adjust the contract. A "mass solution" may have to be worked out if many contracts are affected. This takes time. If the company itself is in a non-whitelisted third country, it must expect to be contacted very quickly by clients who expect a solution for the introduction of the new SCCs as well as support in carrying out the TIA (question 41). Here, the company must prepare well in advance.
  - The second group includes those cases where services are procured from one of the large well-known providers who use standardised contracts (example: cloud providers such as Microsoft, Amazon, Salesforce.com). Here, it is usually easiest to wait for a proposal for action from the provider. If nothing happens, you should ask. Most providers will develop a standard procedure; otherwise the flood of adjustments would not be manageable.
  - The third group of cases is sorted by risk. This refers to the risk associated with the data and the processing (due to the nature, scope or purpose of the processing). Data exports to the US tend to have a higher priority than data exports

to other non-whitelisted third countries such as India.[32] Processors receive a higher priority than other controllers.[33]

- The entries of the third group are processed according to their priority and it is examined whether they require the new SCCs (because they already relied on the SCCs in the past or the previous legal basis such as Privacy Shield has ceased to exist).
- If the new SCCs are required, the importer (e.g. the service provider) is written to and asked for two things:
  - Information on the risk of access by the authorities without a guarantee of legal recourse (c.f. question 40). At the same time, it should be asked for proposals to reduce this risk through further measures. It can be assumed that particularly service providers with many clients will receive large numbers of requests and will refuse to fill out questionnaires. Instead, they will refer to standard answers with the required information.
  - Signing of a contract document which replaces the previous SCCs with the new SCCs, whereby this can either already be filled in with the information required for the Appendix or this can be left to the importer.
- Based on the information regarding the risk of access by the authorities without a guarantee of legal recourse, a TIA is used to check whether the risk is justifiable (point 41). If it is, it will be signed. If further measures are possible, they are evaluated and agreed upon if necessary. This process must be completed by the time the data processing is changed (e.g. ordering additional services, covering additional locations), but no later than December 27, 2022.
- With a view to the period after September 27, 2021, the company's own contract templates will be adapted to replace references to or the use of the previous SCCs. This also applies to their own standard contracts that refer to the SCCs.

As far as data exports from Switzerland are concerned, it is advisable to wait until it is clear what the FDPIC's position is on the new SCCs before signing or sending contract forms to third parties.

---

32 Because, for whatever reason, EU data protection authorities consider the US jurisdiction to be particularly dangerous.

33 In the US, they tend to be covered by laws that provide for access to authorities without a guarantee of legal recourse.

46. What do we have to consider when creating or examining an IGDTA?

An IGDTA is, in concept, a multi-party contract that some or all of the companies in a group of companies conclude with each other in order to regulate the data flows within this group in a data protection-compliant manner.

In practice, we see IGDTA of very different scope and quality. In the early days, IGDTA only regulated international data transfers to non-whitelisted third countries by agreeing on SCCs on all sides. Nowadays, IGDTAs usually also regulate data processing arrangements within the group.

The IGDTA we have drawn up for our clients also cover the requirements of Art. 26 GDPR (joint controllerships), provide for intra-group representation (under Art. 27 GDPR and UK GDPR) and regulate the monitoring and administration of the IGDTA. Also, they cover for the fact that the UK has not yet accepted the new SCC and govern the transition from existing IGDTA. These contracts are at first sight often rather complex, but they have the advantage of covering many of the applicable requirements in one contract and uniform regulations.

Some points to check an IGDTA for:

- In addition to data transfers to non-whitelisted third countries, are intra-group order processing also regulated?
- Are the special cases of Switzerland and the UK covered?
- Are onward transfers from non-whitelisted third countries regulated in addition to data transfers from the EEA and whitelisted third countries?
- Have the gaps in the SCC been filled adequately?
- Are data transfers from non-European countries with data protection laws also covered by the IGDTA?
- Are country-specific adaptations possible and have they been made where needed?
- Have provisions been made for those data transfers that were forgotten or not taken into account when the SCC were issued?
- Do the SCC also apply where an exporter is not in the EEA or a whitelisted third country, but data protection law (such as the GDPR) requires safeguards?
- Does the IGDTA allow for a transfer to an non-whitelisted third country also on the basis of the exceptions (e.g. Art. 49 GDPR)?
- Are controller-to-controller transfers within the EEA and whitelisted countries covered?

- Does the IGDTA work for transfers that are subject to a data protection law that is not the GDPR?
- Are the necessary internal group delegations (e.g. information of data subjects) regulated?
- Is the involvement of external service providers regulated? Do they have their own data security requirements? Are they listed?
- Are data transfers within the EEA and secure third countries regulated?
- Are cross-border data transfers within a legal entity (e.g. from the parent company to a branch and vice versa) to non-whitelisted third countries covered?
- Is the smooth replacement of an existing IGDTA envisaged and adequately regulated? Is the continuation of the existing SCCs in countries where the new SCCs are not yet recognised ensured?
- Are regulations on collective work agreements and works councils in place (important for Germany)?
- Are there sufficient regulations for joint controllerships (Art. 26 GDPR)?
- Are there intra-group arrangements for the purposes of complying with Art. 27 GDPR (and comparable provisions in other data protection laws)?
- Can the IGDTA be easily adapted without repapering?
- Is the information of the parties about developments under the IGDTA regulated in a practical manner?
- Is the applicable law and jurisdiction regulated appropriately and in accordance with the GDPR - both in the IGDTA and in the SCC?
- Is it clear who is responsible for the administration of the IGDTA?
- Is it easy for parties to join and leave at any time?
- Does the IGDTA contain the necessary additional information about the parties as required under the new SCC?
- Is it clear which supervisory authority is responsible for which party – including in the case of non-GDPR jurisdictions?
- Are the data transfers sufficiently detailed? Are all data transfers covered?
- Is it clear which companies are involved in which data transfers and in which role?
- Are the technical and organisational data security measures described in more than just generic terms as seen very often in the past? Do they cover more than just data security, but also, for example, processing principles and data subjects' rights?

If an IGDTA already exists, we recommend a gradual replacement. Unfortunately, it is not possible to update an existing IGDTA by simply replacing the old SCC in the annex with the new SCC one. In order for the new SCCs to function properly, more adjustments are necessary. As our experience shows, the annexes often have to be expanded considerably.