

www.jusletter-it.eu

Daniel Ronzani

The New Standard Contractual Clauses in Practice

Category of articles: TechLawNews by Ronzani Schlauri Attorneys

Region: Switzerland

Field of law: LegalTech

Citation: Daniel Ronzani, The New Standard Contractual Clauses in Practice, in: Jusletter IT
16 December 2021

[1] The old Standard Contractual Clauses (SCC) used under the repealed Privacy Shield regime have been revised.¹ In this article I review them from a practical perspective.

[2] The new SCC for transfer of personally identifiable information (PII) to so called inadequate countries² were implemented by decision of the European Commission on 4.6.2021³. The Swiss Federal Data Protection and Information Commissioner (FDPIC) recognised the new SCC *with reservation* on 27.8.2021⁴ as the basis for PII transfers to countries without adequate level of data protection⁵, provided that the necessary adaptations and amendments were made for use under Swiss data protection law. In either case the old SCC *must be replaced* by the end of 2022.

[3] In a nutshell:

- 1) The SCC cannot be adopted in their entirety. The applicable modules⁶ need to be selected (either by reference or by copy-pasting into a new document).
- 2) The SCC may not be amended/changed (subject to selection of one or several of the four modules and specifically foreseen options).
- 3) Separate data processing agreements under art. 28 (3) GDPR are no longer required as the new SCC cover those terms as well.
- 4) As already noted by Simon Schlauri, the SCC advocate a *risk-based approach*. However, the parties must *warrant* they have no reason to believe that in the destination country (e.g. USA) foreign access exists without any guarantee of legal recourse, and if a foreign authority does attempt to access the data, they must inform the data subject and try to prevent the access.
- 5) The parties need to ensure compliance despite the importer's domestic law and document their assessment in a transfer impact assessment (TIA)⁷. In essence, the TIA clarifies whether the data importer can be compelled by the local authority to hand over PII and whether such lawful access fails to meet standards of EU / Swiss law. Despite performing a TIA, the parties will likely need to implement additional technical and organisational measures to protect the (exported) PII, for instance by on-device-encryption.⁸
- 6) Finally, in addition to the TIA, the FDPIC recommends requesting a separate questionnaire from US providers (and their subcontractors). It is specifically drafted for PII transfers to the USA. It relates to the direct application of 50 U.S.C. § 1881a (FISA 702)⁹ and the indirect enforcement of FISA 702.¹⁰

¹ Cf. in this Jusletter IT edition SIMON SCHLAURI, Die sogenannte «Treuhändlung» für das Schrems-II-Urteil.

² EC Adequacy Decisions, tinyurl.com/5n98r254.

³ EC Implementing Decision EU 2021/914 (tinyurl.com/2p9xbrjy).

⁴ FDPIC: The transfer of personal data to a country with an inadequate level of data protection based on recognized standard contractual clauses and model contracts, tinyurl.com/2p96mwfv.

⁵ Swiss country list by FDPIC, tinyurl.com/bdfsjxms.

⁶ Transfer types: controller-controller, controller-processor, processor-processor, and/or processor-controller.

⁷ IAPP TIA template, tinyurl.com/mcs56kvr.

⁸ Cf. FN 1.

⁹ Cf. tinyurl.com/432bdssu.

¹⁰ FDPIC, Guide to Checking the Admissibility of Direct or Indirect Data Transfers to Foreign Countries (art. 6 (2)(a) FADP), cf. the annex in the end of the document.

[4] It is important to note that merely signing the SCC will *not* suffice. As noted above, the parties need to assess the data protection risk (TIA) and also implement the necessary technical and organizational measures (TOMs).

[5] Given that two regimes apply (EU and Swiss), some clarifications are necessary according to the FDPIC¹¹:

- The FDPIC is the supervisory authority if the PII transfer is exclusively under Swiss law. Parallel supervision by the FDPIC and the EU Supervisory Authority is permissible if the PII transfer is under FADP and GDPR (Clause 13 SCC).
- The parties may select the applicable law to be either Swiss or EU (Clause 17 SCC).
- Place of jurisdiction is a free choice, however, the SCC must be supplemented specifying that data subjects are not excluded from filing claims in their place of habitual residence (i.e. Switzerland) (Clause 18 SCC).
- A clarification is necessary to ensure that references to the GDPR are inclusive of the FADP.
- Until the revised FADP comes into force, the SCC must also cover Swiss legal entities as entitled data subjects (art. 3 lit. b FADP).

[6] The implementation of the SCC requires a thorough analysis of all parties involved. The four modules can be applied and combined in many different ways. Completion of the TIA requires a robust understanding of the technical setup, including the TOMs, and ideally support by US attorneys. I recommend that both exporter and importer each complete a TIA. A comparison of the results might yield discrepancies in the technical and legal understanding and protection of the PII on the importer's platform, in which case they should be ironed out prior to any data export.

¹¹ For details, please refer to the table in s. 4.3.1 of FN 4.