BÄR & KARRER

BRIEFING SEPTEMBER 2021

# SWITZERLAND RECOGNISES THE EU STANDARD CONTRACTUAL CLAUSES. ARE SWISS DATA EXPORTERS NOW SAFE AGAIN?

**On August 27, 2021, the Swiss Federal Data Protection and Information Commissioner (FDPIC) recognised the revised EU standard contractual clauses (SCC) published on June 4, 2021 as contractual safeguards (see our Briefing from June 2021) for transfers of personal data by Swiss companies to countries without an adequate level of data protection, provided that some amendments as specified by the FDPIC are made (see the FDPIC's communication of August 27, 2021). Swiss companies currently relying on SCC to transfer personal data abroad will need to adopt the new SCC by December 31, 2022 at the latest.**

## IS THERE A GRACE PERIOD FOR COMPANIES TO ADOPT THE NEW SCC?

Until December 31, 2022, Swiss companies may still rely on the old SCC for continued and not significantly changed data exports, provided that the SCC were entered into prior to September 27, 2021. After the latter date, the old SCC may not be entered into anymore. We recommend to cease using the old SCC and to replace any existing SCC with the new SCC if no other safeguards are available for data exports after September 27, 2021.

## WHAT ADAPTATIONS TO THE SCC ARE REQUIRED FOR USE IN SWITZERLAND?

The new SCC include four modules representing different data export scenarios:

> **Module 1:** For controller-to-controller data exports
> **Module 2:** For controller-to-processor data exports
> **Module 3:** For processor-to-processor data exports
> **Module 4:** For processor-to-controller data exports

*https://media.baerkarrer.ch/karmarun/image/upload/baer-karrer/xh8ertunm6frwp2gjymp.pdf*

*https://www.edoeb.admin.ch/dam/edoeb/en/dokumente/2021/Paper%20SCC%20def.en%2024082021.pdf.download.pdf/Paper%20SCC%20def.en%2024082021.pdf*

*https://www.edoeb.admin.ch/dam/edoeb/en/dokumente/2021/Anleitung%20f%C3%BCr%20die%20Pr%C3%BCfung%20von%20Daten%C3%BCbermittlungen%20mit%20Auslandbezug%20EN.pdf.download.pdf/Anleitung%20f%C3%BCr%20die%20Pr%C3%BCfung%20von%20Daten%C3%BCbermittlungen%20mit%20Auslandbezug%20EN.pdf*

As a first step, the data exporting Swiss company must now select the appropriate module in each specific case and then analyse whether the envisaged data transfer is subject to: (i) only the FADP or (ii) both the FADP and the GDPR. The data exporter should continue by making the following (minor) amendments to the new SCC:

> The SCC must include the protection of the data of legal entities until the revised Swiss Federal Act on Data Protection („Revised FADP") enters into force (expected to be on January 1, 2023, as the FDPIC indicated in its communication of August 27, 2021).

> The term „member state" in the SCC should include Switzerland or be replaced accordingly, e.g. with „jurisdiction" to ensure that Swiss data subjects can claim their rights in Switzerland.

> References to the GDPR need to be understood as references to the FADP (if only the FADP applies) or to the FADP insofar as the data exports relate to personal data also protected under the FADP (if both the FADP and the GDPR apply).

> The FDPIC must be the exclusive supervisory authority (if only the FADP applies) or be competent to supervise the data exports governed by the FADP (if both the FADP and the GDPR apply).

Furthermore, the SCC provisions relating to the applicable law and the place of jurisdiction must be adapted (how to do this depends on whether only the FADP or also the GDPR applies).

## DO SWISS COMPANIES NEED TO PERFORM A TRANSFER IMPACT ASSESSMENT („TIA")?

Yes, the FDPIC stresses in its communication of August 27, 2021 that Swiss companies need to assess on a case-by-case basis whether contractual clauses are actually suitable for ensuring appropriate protection of the transferred personal data or whether supplementary measures need to be in place in addition to the SCC.

As set out in the FDPIC's guide of June 2021 to checking the admissibility of direct or indirect data transfers to foreign countries, the data exporter needs to evaluate on a case-by-case basis whether the laws in the receiving country relating to lawful data access by foreign public authorities (e.g. for national security or criminal investigation purposes) and data subject rights are compatible with Swiss data protection law and Swiss constitutional principles. In particular, to be compatible, the foreign law must provide the following four guarantees: (i) a clear legal basis for such lawful data access, (ii) the authorities' powers and measures must be suitable and necessary to fulfil the legal purposes of their access, (iii) data subjects in Switzerland must have effective legal remedies to enforce their rights to privacy (e.g. rights of access, rectification and deletion), and (iv) legal recourse as well as access to an independent, impartial court must be possible.

If the data exporter concludes that the third country provides these four guarantees, the SCC can be entered into and will provide an adequate level of data protection. Otherwise, the data exporter must take additional measures to ensure that transferred data is adequately protected. These may be of a contractual, technical or organisational nature (see our Briefing from June 2021).

## ARE THERE ALTERNATIVES TO REPLACING THE OLD SCC WITH THE NEW SCC?

SCC are only one option to provide sufficient safeguards for transfers of personal data to countries without an adequate level of data protection. Other options which Swiss companies may consider include binding corporate rules („BCRs") for group-internal data transfers or individual contractual clauses. These, however, require a case-by-case examination and approval by the FDPIC and are therefore more burdensome. Furthermore, Swiss companies which transfer personal data abroad in order to fulfil their contractual duties towards their customers do not need to sign SCC or implement BCRs for such transfers (e.g. a travel agency that shares the name and contact details of a customer with the hotel the customer has booked).

In practice, as in the past, we expect the new SCC to be the most relevant basis for cross-border data transfers from Switzerland to third countries without an adequate level of data protection.

## DOES THE USE OF THE NEW SCC STILL NEED TO BE NOTIFIED TO THE FDPIC?

Data transfers based on the new SCC must still be notified to the FDPIC until the Revised FADP enters into force. The same applies if parties decide to enter into the old SCC until September 27, 2021. However, if the new or old SCC are used, a simple notification letter to the FDPIC is sufficient, and no case-by-case examination by the FDPIC is required. Even though this question is not explicitly addressed in the FDPIC's communication of August 27, 2021, Swiss companies which have previously informed the FDPIC about their use of the old SCC are advised to again inform the FDPIC after having implemented the new SCC.

## Authors

**Corrado Rampini**
Partner
T +41 58 261 52 83
E corrado.rampini@baerkarrer.ch

Corrado Rampini heads the real estate practice and the data privacy practice of Bär & Karrer. He advises Swiss and international companies and organizations in all privacy related matters. He commented the provisions applicable to private institutions in a leading commentary of the Swiss data protection law.

**Christian Kunz**
Counsel
T +41 58 261 52 66
E christian.kunz@baerkarrer.ch

Christian Kunz advises clients in the field of data and technology law (including data strategies, outsourcings, international data transfers, cross-border disclosure requests and issues of Swiss and European data protection law) and conducts international investigations and e-discovery projects. He also regularly advises in private M&A transactions and on general corporate, corporate governance and commercial matters.

**Rehana Harasgama**
Associate
T +41 58 261 54 51
E rehana.harasgama@baerkarrer.ch

Rehana Harasgama is an expert in domestic and international data protection law and advises clients on complex data protection and privacy questions, such as major cross-border disclosure requests, the adoption and implementation of privacy-by-design in new technologies and business models, the implementation of data breach response plans and the handling of employee personal data.