

N

Monthly
Newsletter
May 2022

Data

Schellenberg
Wittmer



Need for Action Regarding Cross-Border Data Transfers

Samuel Klaus, Roland Mathys, Kenzo Thomann

Key Take-aways

- 1.** For cross-border data transfers, the new EU-SCC (*Standard Contractual Clauses*) with adaptations to Swiss law (*Swiss Rider*) must be used - under both the current and revised Swiss Data Protection Act.
- 2.** Existing SCC must be replaced by new EU-SCC with Swiss Rider by the end of 2022, including performing (and documenting) a risk assessment (*Transfer Impact Assessment; TIA*).
- 3.** Until the revised Swiss Data Protection Act comes into force, the conclusion of new SCC must be notified. Failure to comply with the notification obligation may result in a fine under the current law.

1 Cross-Border Data Transfers and the New SCC

In many business transactions (inter-company and external), personal data located in Switzerland is either transferred to parties outside of Switzerland or accessible by parties outside Switzerland, e.g. when using cloud services.

If the country of the receiving (or accessing) party does not offer a sufficient level of data protection (from a Swiss perspective), the Swiss Data Protection Act (**DPA**) requires that this be compensated for by protective measures (Art. 6 para. 2 DPA). In practice, this is mostly done by so-called **Standard Contractual Clauses (SCC)**. SCC are officially formulated or recognized agreements that are concluded between the data exporter and the data importer and serve to secure the data transfer with protective contractual provisions. SCC are already necessary under the current DPA and will continue to be so under the revised DPA (**revDPA**).

The commonly used EU Standard Contractual Clauses (**EU-SCC**) were revised in 2021, and since September 2021 only these new EU-SCC may be used for new data transfers. The Federal Data Protection and Information Commissioner (**FDPIC**) has also recognized the EU-SCC for Switzerland, provided they are adapted to Swiss data protection law (see section 4 below). If the EU-SCC are to be used for data transfers from Switzerland, the **new EU-SCC** must be used and must be **adapted to Swiss data protection law** (with a "**Swiss Rider**"). Existing SCC based on the "old" EU-SCC may remain in use until December 31, 2022, provided there are no significant changes to the data transfers in question. **Before the end of 2022, however, they must be replaced on the basis of the new EU-SCC with the necessary adaptations to Swiss law.**

When concluding new SCC, the EU-SCC must be amended with a Swiss Rider.

2 When are SCC Required?

2.1 Lack of Adequate Level of Data Protection

SCC (or other protective measures according to Art. 6 para. 2 DPA, which are not addressed herein) are necessary if data is transferred to a country (or if such data is accessed from a country) **which lacks an adequate level of data protection**. Information on this can be found in the country list published by the FDPIC (and under the revDPA by the Federal Council). The EU/EEA member states provide a sufficient level of data protection for **personal data pertaining to individuals**, however, not for personal data pertaining to legal entities.

The USA (where a relevant number of cloud and SaaS service providers are located) is not deemed to provide a sufficient level of data protection for any personal data.

It should also be noted that under current Swiss data protection law, **personal data pertaining to legal entities** is also covered by the DPA, which is not the case under the data protection laws of the EU/EEA member states. The **EU/EEA member states are thus not considered "secure" destinations** (from the perspective of the DPA) for personal data pertaining to legal entities. This will change however, when the revDPA comes into force (expected on September 1, 2023): The revDPA will only apply to personal data pertaining to individuals, personal data pertaining to legal entities will no longer be in scope. **Until the revDPA comes into force, data transfers with personal data pertaining to legal entities must continue to be secured by means of SCC for data transfers to (or accessibility from) EU/EEA member states.**

The effort required to replace existing SCC should not be underestimated.

2.2 SCC for Contractual Relations and Within the Corporate Group

The data exporter is responsible for protecting data transfers to those countries deemed under Swiss law to have insufficient data protection by concluding SCC with the data importer. Usually, this is done by means of a corresponding obligation in the main contract (e.g., the cloud or SaaS service contract) with the **SCC as an annex** or a side contract to be concluded in parallel to the main contract.

The obligations regarding SCC are **also applicable within a corporate group**. If data is transferred within a group, e.g. from a Swiss subsidiary to a group company in the USA, protective measures will be required. In practice, SCC are used here as well, as part of a more comprehensive internal group wide agreement on data transfers (so-called **Intra-Group Data Transfer Agreement; IGDTA**).

2.3 Example: Cloud or SaaS Services From a US Provider

In practice, it is often the case that a Swiss company wants to use certain services e.g. cloud or SaaS services offered by a US provider, whereby personal data under the responsibility of the Swiss company is stored on servers in the USA (or whereby at least access is granted from the USA, e.g. for support purposes). Since the USA does not offer an adequate level of data protection from the perspective of Swiss data protection law, such data transfers must be secured by SCC.

International providers of cloud or SaaS services usually already have appropriate **SCC templates** which they offer to con-

clude with their European customers. From a Swiss perspective, it must thereby be ensured that such templates, which usually only take into account the EU-SCC, also contain the **appropriate additions under Swiss law**, as required by the FDPIC.

3 Specific Need for Action

3.1 New Cross-Border Data Transfers

If new cross-border data transfers are made, e.g. as part of new business processes or when using new service providers, it must be clarified whether this leads to data transfers to countries with an inadequate level of data protection. If this is the case, then (unless any other exemption under Art. 6 para. 2 DPA is applicable) new **EU-SCC** should be concluded, with the appropriate **amendments according to Swiss data protection law (Swiss Rider)**.

The SCC are modular in structure, and the appropriate **modules** are to be selected depending on the specific situation and the role of the involved parties as data controllers or processors. Certain clauses also offer **individual options to be chosen**, and specific information on the data transfer and the technical and organizational measures in question must be provided in the **annexes**. The SCC should be adapted and the annexes completed in close coordination between Business/Operation and Legal/Compliance.

3.2 Replacing Existing SCC

If there are already SCC in place, it should be monitored whether the underlying data transfers change significantly. This may be the case, for example, if business processes are adapted or data processing is expanded. If such a **significant change** occurs, the corresponding SCC must be replaced in advance with new SCC based on the new EU-SCC (with a Swiss Rider).

Even if no significant change to data processing is planned in the next few months, there is still a **need for action: the existing SCC must be replaced with new EU-SCC (with a Swiss Rider) by December 31, 2022**. To do so, an overview of existing SCC is required. Once it has been determined which SCC need to be replaced, sufficient time should be allocated to do so. It may be helpful to involve external service providers for the implementation.

In practice, it has proven useful to first prepare an **overview** of data recipients and their contact persons. If it becomes apparent that a number of SCC need to be replaced, **prioritizing** them might be helpful (e.g., according to the sensitivity of the affected data), and creating a general **"cover sheet"** for the EU-SCC, which contains the general SCC adjustments as well as the individual SCC adjustments per data recipient.

Even though the SCC are to a large part standardized, the **effort required for their conclusion with each data recipient concerned** should not be underestimated - especially for companies that rely on numerous service providers. If a large number of SCC need to be replaced, alternative mechanisms could be considered (such as e.g. unilateral information of the data recipient with reference to the newly applicable SCC). Whether this can be a viable option under the specific circumstances should be examined in detail in each case and by means of an appropriate risk assessment.

3.3 Transfer Impact Assessment Requirement

The new EU-SCC stipulate that a so-called **Transfer Impact Assessment (TIA)** must be carried out (clause 14 of the EU-SCC). The TIA is a **risk assessment** to examine whether the data importer may be forced to violate the provisions of the SCC due to local regulations. The result of this assessment must be **documented**.

Experience has shown that this relatively new requirement leads to some **clarification needs and additional effort regarding implementation**. Such a risk assessment cannot be carried out in a general or company-wide manner, but must take into account the circumstances of the specific individual case, i.e. the relevant data transfer concerned.

**Until the revDPA
comes into force, the
notification obligation
must be complied with.**

4 What Does the "Swiss Rider" Contain?

The FDPIC has indicated which aspects a **"Swiss Rider" to the EU-SCC** must contain in order for the EU-SCC to also comply with Swiss data protection law. Such a Swiss Rider must contain, *inter alia*, provisions on the competent supervisory authority, the applicable law, the place of jurisdiction, and for personal data pertaining to legal entities (see section 2.1 above).

There are **three options** available, depending on whether a data transfer is exclusively subject to the DPA (option 1) or whether the EU General Data Protection Regulation (**GDPR**) also applies simultaneously (option 2). In the latter case, the SCC can either be adapted in such a way that each data transfer is treated individually based on the regulation applicable as per the relevant data protection law, i.e. DPA or GDPR (option 2a), or the GDPR standard can be selected to apply to all data transfers (option 2b).

Which option is most appropriate depends on the circumstances of the individual case. In particular, if within a larger group the Swiss companies are already compliant with the GDPR requirements, choosing option 2b may facilitate and help to standardize internal processes.

5 The Notification Obligation - and its Impending End Under the Revised DPA

Under the current DPA, **the FDPIC must be notified regarding the use of SCC** before a cross-border data transfer may take place (Art. 6 para. 3 DPA). A generic notification by the data exporter stating that EU-SCC (adapted to Swiss data

protection law) are being used, will suffice. The SCC do not have to be disclosed and no specific approval by the FDPIC is required. Violations of the notification obligation can be sanctioned under criminal law with a fine of up to CHF 10,000 (Art. 34 para. 2 lit. a DPA).

Under the revDPA, this notification obligation will no longer apply. Until the coming into force of the revDPA (currently expected per September 1, 2023) however, this notification obligation still needs to be complied with.

6 Conclusion

In case of cross-border data transfers (or the granting of access from abroad to data in Switzerland), it must be verified whether the level of data protection in the destination country (or the country from which data is accessed) meets the requirements of Swiss data protection law. If this is not the case, in particular also regarding EU/EEA member states in case of personal data pertaining to legal entities, SCC must be concluded on the basis of the new EU-SCC with an appropriate Swiss Rider.

Existing SCC may continue to be used until the end of 2022 however, they must be replaced with new SCC by December 31, 2022. The necessary effort for implementation should not be underestimated. It is therefore advisable to initiate the review as to whether and to what extent new SCC need to be concluded at an early stage.



Roland Mathys
Partner Zurich
roland.mathys@swlegal.ch



Dr. Samuel Klaus
Partner Zurich
samuel.klaus@swlegal.ch



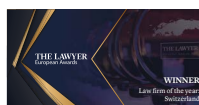
Vincent Carron
Partner Geneva
vincent.carron@swlegal.ch



Dr. Catherine Weniger
Counsel Geneva
catherine.weniger@swlegal.ch

The content of this Newsletter does not constitute legal or tax advice and may not be relied upon as such. Should you seek advice with regard to your specific circumstances, please contact your Schellenberg Wittmer liaison or one of the persons mentioned above.

Schellenberg Wittmer Ltd is your leading Swiss business law firm with more than 150 lawyers in Zurich and Geneva, and an office in Singapore. We take care of all your legal needs – transactions, advisory, disputes.



Schellenberg Wittmer Ltd
Attorneys at Law

Zurich
Löwenstrasse 19
P.O. Box 2201
8021 Zurich / Switzerland
T +41 44 215 5252
www.swlegal.ch

Geneva
15bis, rue des Alpes
P.O. Box 2088
1211 Geneva 1 / Switzerland
T +41 22 707 8000
www.swlegal.ch

Singapore
Schellenberg Wittmer Pte Ltd
6 Battery Road, #37-02
Singapore 049909
T +65 6580 2240
www.swlegal.sg