BÄR & KARRER

BRIEFING JUNE 2021

CROSS-BORDER DATA TRANSFERS: THE REVISED STANDARD CONTRACTUAL CLAUSES ARE OUT. IS THIS THE END OF THE HIATUS?

On 4 June 2021, the European Commission („Commission") finally published the revised Standard Contractual Clauses („SCCs") which companies have been expecting for almost a year. Following what privacy activists called the "big win" for data protection in the EU, the Court of Justice of the European Union („CJEU") left companies relying on the so-called Privacy Shield or the SCCs in force at that time for cross-border data transfers from the EU to the US in limbo: Last July, the CJEU invalidated the Privacy Shield as a transfer mechanism to the US in its Schrems II ruling and, while it confirmed that SCCs could still be used for such cross-border transfers to the US, the CJEU put an end to companies just signing them and not giving them a second thought. Companies were from then on required to conduct a data transfer impact assessment („DTIA") to assess the risks of government access to personal data transferred to the US, and they had to implement supplementary measures to protect the transferred data. The Swiss Federal Data Protection and Information Commissioner („FDPIC") followed suit. At the same time, the Commission announced that it would be giving the SCCs a major overhaul, in particular to address some of the issues of the Schrems II ruling. This BK Briefing discusses what the revised SCCs actually entail for companies transferring personal data to third countries, in particular to the US.

BACKGROUND

Under the EU's General Data Protection Regulation („**GDPR**"), the SCCs provide appropriate safeguards for transfers of personal data to a third country or international organisation without an adequate level of data protection (art. 46 para. 2 lit. d).

The FDPIC also recognised the previous version of the SCCs as offering sufficient safeguards for cross-border data transfers to such third countries from Switzerland under art. 6 para. 2 lit. a of the Swiss Federal Act on Data Protection („**FADP**") and it is expected that the FDPIC will do the same again for the revised SCCs.

As described above, since the CJEU's *Schrems II* ruling of 16 July 2020, data importers and exporters have faced significant legal uncertainty when transferring personal data to third countries, in particular the US, given that SCCs as data importers and exporters had to verify, on a case-by-case basis, whether the law in the recipient country ensures adequate protection for personal data transferred under SCCs and, where it does not (e.g. due to national security laws), provide additional safeguards or suspend cross-border transfers (see our BK Briefings regarding the effects of the *Schrems II* ruling from July and September 2020). After the *Schrems II* ruling, companies at least knew the answer to this question for cross-border data transfers to the US. The FDPIC followed the CJEU's view and added the same caveat for binding corporate rules.

https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc/standard-contractual-clauses-international-transfers_en

https://www.baerkarrer.ch/de/publications/the-end-of-the-privacy-shield-juggling-the-requirements-for-cross-border-data-transfers-to-the-us

https://www.baerkarrer.ch/de/publications/inadequacy-of-the-swiss-u.s.-privacy-shield-filling-the-gaps-around-the-federal-data-protection-and-information-commissioners-opinion-on-cross-border-data-transfers-to-third-countries

The revised SCCs now aim to eliminate this legal uncertainty. However, the Commission stated that companies will still need to implement supplementary measures when transferring personal data to countries that do not pass the DTIA, e.g., because the local government may have a right to access the transferred personal data. Consequently, a certain degree of legal uncertainty still remains, and companies will have to continue to conduct DTIAs before transferring personal data to third countries. The implementing decision of the Commission will be effective 20 days after it has been published in the Official Journal of the EU and the revised SCCs can be used from then onwards.

KEY CHANGES

The Commission has substantially revised the SCCs. Key changes in the SCCs include:

- The SCCs adopt a **modular approach** enabling data exporters and importers to **select the clauses that are relevant to the type of data transfer** they engage in (processor-to-processor and processor-to-controller transfers, in addition to controller-to-controller and controller-to-processors transfers included in the previous SCCs).
- The SCCs include **clauses applicable to all data transfers, followed by four different modules of specific terms for each type of transfer.**
- The SCCs establish a **data importer and exporter duty to evaluate the laws of the receiving country:** As previously, the SCCs require not only the data importer, but also the data exporter, to warrant that it has no reason to believe that the **laws and practices** of the recipient country, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under the SCCs.
  However, the SCCs now specify that, in providing this warranty, the parties must declare that they have considered not only the specifics of the data transfer but also the laws and practices of the recipient country that are relevant in light of the circumstances of the transfer (**risk-based approach**). As a result, the parties are required to **conduct a DTIA** which, among others, takes into consideration the following elements: the length of the processing chain, the number of actors involved, the transmission channels used, the categories and format of the transferred personal data and the economic sector in which the transfer occurs. As regards the impact of such laws and practices, the parties may also consider **case law**, reports by oversight bodies and other reliable information on **how the law is applied in practice**, the **existence or absence of requests** in the same sector and, under strict conditions, the **own documented practical experience** of the data exporter and/or importer with prior instances of requests for disclosure from public authorities, or the absence of such requests.
  The data importer must also, if it becomes aware that it cannot fulfil its obligations, **promptly notify the exporter**, and the exporter must **implement additional measures**. If there are no appropriate measures or if instructed to do so by the data protection authority, the exporter must **suspend the transfer** and is entitled to terminate the contract.
- The SCCs provide for **extended data importer obligations in connection with government access requests:** Under the revised SCCs, in case of a government access request for disclosure of personal data, or a data importer becoming aware of any direct access to such data by public authorities, the data importer (as processor or controller) is not only obliged to notify the data exporter (and, where possible, any affected data subject), but also, if the importer is **prohibited from notifying the data exporter, to use its best efforts to obtain a waiver on the prohibition.**The data importer must also **regularly update the data exporter on requests received** and keep such information on file in case requested by data protection authorities. Furthermore, the data importer must **review the legality** of such disclosure requests, **provide the minimum information permissible** in response to such disclosure requests and **exhaust all available remedies to challenge the request, including seeking interim measures**, if, after a careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the recipient country.
- In addition, the revised SCCs establish:
  - **Stricter onward transfer restrictions.**
  - **New transparency requirements**, e.g., in a controller-to-controller set-up, data importers must provide notice regarding their data processing activities similar to the requirements under GDPR.
  - **More detailed security measures**, e.g., data

importers and exporters may need to provide more extensive information about the technical and organizational measures they have in place — in particular, as they relate to data security.

Overall, under the revised SCCs, data importers and data exporters have greater responsibilities when it comes to assessing the level of data protection in the recipient country. Data exporters have to rely on the information they receive from the data importers with regard to any potential laws and practices that may prevent an adequate level of data protection even under the SCCs. Moreover, data importers have greater burdens when it comes to averting government access and its information duties toward the data exporters (e.g., to obtain a waiver on the prohibition to notify the data exporter and to exhaust all available remedies to challenge a disclosure request, data importers may need to take legal action).

WHAT DOES THIS MEAN FOR DATA TRANSFERS TO THE US?

Whether the SCCs provide sufficient safeguards for a transfer of personal data from Switzerland to the US mainly depends on how the parties assess the risk of the data importer being required to disclose personal data based on a government access request.

In practice, we expect that parties may in some cases be unable to rate the risk as low or to exclude any such risk so that even the revised SCCs may, without supplementary measures, in such cases not provide sufficient safeguards for a transfer of personal data to the US.

Possible solutions which are worth further assessment in each specific case include:

- Encryption of the data by the data exporter prior to the transfer to exclude clear data access by the data importer (without sharing the encryption key, e.g., bring your own key).
- Protective orders.
- Confidentiality undertakings.
- Remote read-only access to data stored on a Swiss-based server (technically exclude download option, and therefore, potentially any direct government access).
- If practically feasible and suitable, obtain the data subject's individual consent for the data transfer.
- Impose a duty on data importer never to provide the transferred personal data to government authorities in the recipient country voluntarily.

WHAT CAN COMPANIES DO TO CONTINUE CROSS-BORDER TRANSFERS TO THE US AND OTHER THIRD COUNTRIES?

As we expect the FDPIC to recognise the revised SCCs as providing sufficient safeguards for cross-border data transfers to third countries, companies in Switzerland and the EU will have to:

- Implement the revised SCCs within 15 months after the current SCCs have been repealed if they want to continue to rely on SCCs for cross-border data transfers. However, we recommend not to wait with implementing the revised SCCs but to **implement them as soon as possible**, in particular for transfers to the US as supplementary measures will also have to be assessed and brought in.
- Implement a **process to conduct a DTIA** before transferring personal data to other third countries to assess whether supplementary measures will need to be implemented.
- Assess **what supplementary measures** are appropriate to ensure an adequate level of data protection in the future.
- If all else fails, assess whether data transfers can be based on **other safeguards or derogations** according to Swiss or EU data protection law (e.g., consent, contractual necessity, legal or administrative proceedings etc.) or – but this may not be practical in many cases – suspend transfers to the US, request that all data be returned and relocate data to Switzerland or the EU.

The European Data Protection Board is expected to issue their amended recommendations on supplementary measures for cross-border data transfers soon. This should provide further guidance on how to assess and implement supplementary measures for cross-border transfers to third countries such as the US.

AUTHORS

Jan Kleiner
Partner
T: +41 58 261 53 84
jan.kleiner@baerkarrer.ch

Jan Kleiner Co-heads our firm's sport, media and data protection practice groups. His practice covers contentious and non-contentious matters in the fields of national and international sports law as well as media, entertainment and data protection law. He furthermore advises clients on technology and telecommunication law matters.

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

Christian Kunz regularly advises Swiss financial institutions, fintechs and other companies in connection with their data strategies, outsourcings and on Swiss and European data protection law issues. Christian also advises on internal investigations, cross-border proceedings, private M&A transactions and general corporate law, corporate governance and commercial law matters

Rehana Harasgama
Senior Associate
T: +41 58 261 54 51
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.

FURTHER CONTRIBUTER:

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