MINTZ

Transferring Personal Data from Europe – Working with the New Standard Contractual Clauses and Getting to Grips with Your Schrems II Assessment

June 04, 2021 | Advisory | By **Cynthia J. Larose**

VIEWPOINT TOPICS

- Privacy & Cybersecurity

RELATED PRACTICES

- Privacy & Cybersecurity

RELATED INDUSTRIES

The European Commission has adopted (at long last) an updated version of the Standard Contractual Clauses (SCCs), bringing this popular data transfer mechanism in line with the GDPR – and, we hope, the ***Schrems II* decision** issued by the Court of Justice of the European Union in July 2020. The SCCs are the most commonly used legal mechanism for transferring personal data from the EEA to non-EEA countries (known as "third countries"), so the new SCCs are very big news for organizations that transfer or receive personal data from the EEA (that is, the European Union plus Norway, Iceland and Liechtenstein). We anticipate that many of our clients will soon adopt the new SCCs as their primary legal mechanism for personal data transfers – which will also require getting to grips with the risk assessment and supplementary measures required by the *Schrems II* decision. **Organizations will need to start using the new SCCS in mid-to-late September 2021 for new transfers, and adopt them by roughly the end of 2022 to cover old transfers (assuming you still have the data).**

Why are the SCCs important?

Most US companies that receive European personal data are aware that the GDPR prohibits the transfer of personal data from the EEA to "third countries" that don't have the benefit of a Commission "adequacy decision" (currently only 12 countries have one) *unless*

- one of the Commission-approved data transfer mechanisms (such as the SCCs) is in place, or
- an express GDPR Art. 49 exception applies – but these exceptions are heavily circumscribed by stringent guidance issued by the European Data Protection Board and are of very limited use.

Given that we are still waiting for the new, additional data transfer mechanisms anticipated by the GDPR, such as Commission-approved privacy certifications and codes of conduct, the SCCs play a fundamental role in making personal data transfers from Europe legal. In many data transfer situations, the SCCs are the only viable option.

When do we need to start using the new SCCs?

The Commission decision adopting the new SCCs will go into effect 20 days after the decision is published in the Official Journal of the European Union (which is published daily on weekdays). Organizations that want to use the SCCs as the legal basis for new data transfers will need to begin using the new form of the SCCs from the date that is three months after their effective date (so assuming the decision is published on June 7, 2021, new transfers would need to be done under the new SCCs starting on September 26, 2021). For transfers that are already subject to the "old" SCCs, in most cases, organizations will have a grace period of approximately 18 months from now to transition from the old SCCs to the new SCCs (so roughly by the end of 2022). Importantly, it appears from the Commission's decision that even if a *transfer* made under the old SCCs is complete, the new SCCs will need to be executed if the data are still being used by the data importer. Furthermore, the *Schrems II* requirements for a risk assessment with respect to national security laws and the adoption of supplemental protective measures to mitigate any risks apply *now*.

What's new (and improved)?

The new SCCs represent a vast improvement over the current SCCs, which were last updated in 2004 (for controller-to-controller transfers) and 2010 (for controller-to-processor transfers). The new SCCs are modular in nature, covering the following data transfer situations:

- Controller to Controller
- Controller to Processor
- Processor to Controller (NEW!)
- Processor to Processor (NEW!)

The new SCCs offer a number of improvements over the old SCCs:

1. By providing for processor-to-controller and processor-to-processor transfers, the Commission has plugged one of the most significant gaps in the old SCCs. Among other industries, the pharmaceutical industry will welcome the new flexibility: US (and other third country) clinical trial sponsors that are not established in Europe will soon be able to use the SCCs to cover routine transfers of EU clinical study data from their European CROs (which are processors).

2. In addition, it is now clear that controllers who are subject to the GDPR but are not established in the EU can sign the SCCs as data exporters. This has been a vexingly unclear matter under the old SCCs, with some data protection authorities maintaining that controllers that are not based in the EU cannot sign as the exporter, despite the fact that a large number of companies have chosen to do exactly that in light of the lack of approved alternatives and the stringent limitations that the European Data Protection Board has placed on consent and other exceptions (the Article 49 derogations).

3. The new SCCs modules that involve processors also cover the requirements of GDPR Article 28, which specifies a list of items that must be addressed in a written contract whenever a controller uses a processor to do anything with personal data. That will significantly streamline controller-processor contracting.

4. The new SCCs spell out the controller's and processor's obligations clearly. Compared to the old SCCs, companies that have limited familiarity with the GDPR – for example, companies that receive EU personal data yet do not themselves fall under the GDPR's territorial jurisdiction – will find it easier to understand their concrete obligations under the new SCCs because the provisions tell them exactly what they have to do.

5. The new SCCs have been carefully drafted to help the parties address the concerns raised by the EU Court of Justice in its July 2020 *Schrems II* decision. That decision cast doubt on the lawfulness of transferring personal data from the EU to the US – and incidentally also raised the bar for many other countries. (Click **here** for a summary of that case.) The due diligence and disclosures required by the new SCC provisions initially may seem disproportionate to companies that believe their personal data transfers face no risk – or an essentially hypothetical and extremely low risk – of access by their country's intelligence agencies. However, the recently published draft guidance of the European Data Protection Board (summary available **here**; full guidance document **here**) makes it clear that US companies (and others) are required to perform a painstaking assessment of that risk and adopt mitigating measures. That said, the Commission has included a footnote that introduces a very welcome pragmatic angle to the assessment (more on that immediately below).

How do the new SCCs help organizations get to grips with the *Schrems II* decision?

The new SCCs turn the *Schrems II* decision's diligence and supplemental measures requirements into a contractual requirement. The exporter and importer must cooperate in the assessment and document their assessment in writing. The written assessment must be available to EU supervisory authorities (i.e., an interested national or regional data protection authority) on request. However, the assessment does not need to be attached to the SCCs as the European Data Protection Board had recommended to the Commission.

In a nutshell, the exporter and importer need to warrant that "they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses" (Clause 14(a)). In making this warranty, the exporter and importer must take into account, among other things, "the laws and practices of the third country of destination – including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards" (Clause 14(b)(ii)). The SCCs include a long footnote explaining that this analysis should not be limited to the letter of the law in the destination country. Instead, ***practical experience can and should be taken into account.***

This critical footnote in the SCCs adds a much needed counterweight to the European Data Protection Board's statement in its **November 2020 guidance on the *Schrems II* decision** that the assessment must not "rely on subjective factors such as the likelihood of public authorities' access to your data in a manner not in line with EU standards." The SCCs' footnote helpfully clarifies that "practical experience" counts as a *relevant, objective* element rather than a subjective element that must be disregarded:

As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies. (Fn 12)

Overall, the new SCCs bring greater clarity and certainty to the rules governing EU-to-third-country data transfers. They stick tightly to the GDPR, while also spelling out specific obligations in a way that is (for the most part) both precise and achievable. While the new SCCs will require much more thought and background work on the part of data exporters and importers, they should result in more robust organizational and technical protections for the data in question, and for the individuals whose data are transferred.

Now that the new SCCs are in their final form, it's time for US data importers to review their transfers and start assessing the risk that the US government could demand access to the personal data. If there's a risk, the importer and exporter will need to adopt supplementary protections that are considered by EU data protection authorities to mitigate the risk and ensure that the personal data are protected to a standard equivalent to that of the GDPR.

How Mintz can help with your Schrems II assessment

Conducting a *Schrems II* assessment is a significant undertaking. Mintz has prepared a detailed guidance note to assist clients in stepping through the analysis and documenting their assessment. Our *Schrems II* guidance note covers the following:

Part 1, Introduction, explains the basic concerns and effects of the *Schrems II* decision.

Part 2, Conducting and Documenting a *Schrems II* Due Diligence Exercise, describes how to perform and document a *Schrems II* due diligence exercise.

Part 3, *Schrems II* Due Diligence Decision Tree, presents a practical due diligence framework for assessing, through a simple multi-step decision tree, whether a particular personal data transfer is at risk of exposure to US intelligence agencies in light of US national security laws.

Part 4, Additional Safeguards, discusses some of the risk mitigation measures recommended by EU data protection authorities, with a focus on the measures that are most likely to be both effective and achievable within many US organizations.

Appendix A contains relevant provisions of the European Commission's draft of the new Standard Contractual Clauses (SCCs).

Appendix B summarizes the key US national security laws that need to be taken into account when exporting personal data from the European Economic Area or United Kingdom to the US. It is designed to be incorporated (if desired) into the written documentation of the *Schrems II* due diligence exercise.

Appendix C, References and Resources, lists sources of additional information about the *Schrems II* decision, guidance issued by European data protection authorities, reference works concerning US national security laws and programs, and other resources that may be helpful for delving further into the matters covered by the guidance note.

We believe that our *Schrems II* guidance note will empower many clients to conduct assessments of routine, lower-risk transfers internally with limited need for outside counsel. However, we would be very happy to assist with assessments and discuss proposed transfers one-on-one, which may be particularly important for complex or higher-risk transfers.

If you have any questions or concerns or would like to obtain a copy of our *Schrems II* guidance note (which we can provide to our clients on a fixed-fee basis), please contact Cynthia Larose (cjlarose@mintz.com).

Authors

Cynthia J. Larose, Member / Co-chair, Privacy & Cybersecurity Practice

Cynthia J. Larose is Chair of the firm's Privacy & Cybersecurity Practice, a Certified Information Privacy Professional-US (CIPP-US), and a Certified Information Privacy Professional-Europe (CIPP-E). She works with clients in various industries to develop comprehensive information security programs on the front end, and provides timely counsel when it becomes necessary to respond to a data breach.

More Viewpoints

European Commission Adopts Final Version of New Data Transfer Agreement (SCCs)

June 4, 2021 | Blog

Read more

Privacy Shield Invalidated by Top EU Court; Standard Contractual Clauses Upheld (But There Are Still Major Challenges Ahead)

July 16, 2020 | Blog

Read more