On June 4, 2021, the European Commission adopted two new sets of standard contractual clauses (SCCs): one for data transfers from data controllers to data processors and one for data transfers from data exporters to data importers in the United States and other third countries. These new clauses update and replace the SCCs adopted in 2001, 2004, and 2010 that many employers currently use to legally transfer human resources (HR) data for employees based in the European Union (EU).
Specifically, the new SCCs reflect the requirements of the EU General Data Protection Regulation (GDPR) and the July 16, 2020, decision of the Court of Justice of the European Union in Schrems II, as well as recommendations made by the European Data Protection Board (EDPB), European Data Protection Supervisor (EDPS), and public comment. The new SCCs will become effective 20 days from the date of their publication in the Official Journal of the European Union. Controllers will remain able to sign the former sets of SCCs for three months after that date, and all former sets will need to be updated to the new template over the next 18 months as a transition period.

New Standard Contractual Clauses for Data Controllers and Processors

The new SCCs for data controllers and data processors comply with Article 28 of the GDPR and are intended for data transfers from data controllers to data processors that are located within the European Economic Area (EEA) or in countries that have been deemed by the European Commission to provide adequate protection to EEA data subjects (Adequate Countries). The controller-to-processor SCCs set forth new requirements that address the security of data processing, the use of sub-processors, international data transfers, data breach notification, and noncompliance with the clauses, among other issues.

One of the major innovations of these updated clauses is that they permit more than two parties to agree to or later join a single set of contractual clauses. This innovation will limit the number of separate contracts employers must implement when switching to or adding new vendors or service providers.

New Standard Contractual Clauses for Data Transfers to Third Countries

The SCCs for data transfers to third countries are intended for data transfers from data exporters to recipients in third countries such as the United States that the European Commission has determined do not provide an adequate level of personal data protection. (The term “third country” refers to any country that is outside of the EU or EEA and is not an Adequate Country.) The third-country SCCs change the format and update the language of the current SCCs so that they comply with the requirements of the GDPR. More importantly, the third-country SCCs include language intended to comply with the obligations set forth in Schrems II. Schrems II requires data exporters and data importers using SCCs to conduct risk assessments to determine whether the laws of the country in which a data importer is located (specifically, the national surveillance laws) provide an adequate level of protection for the personal data and fundamental rights of data subjects—and if the laws do not, to implement technical, contractual, and organizational supplementary measures to ensure an adequate level of protection for the personal data and fundamental rights of data subjects.

Specifically, the key elements of the third-country SCCs include the following:

Modular Format
A modular format that allows the parties to select appropriate clauses for controller to controller transfers, controller to processor transfers, processor to processor transfers, and processor to controller transfers;

*Multiple-Party Agreements*

The ability for more than two parties to agree to or later join a single set of contractual clauses (similar to the process adopted in controller-to-processor SCCs), thereby limiting the number of separate contracts employers must implement when switching or adding new vendors or service providers, or facilitating onward transfers;

*Technical and Organizational Measures*

An obligation that clauses be drafted to include technical and organizational measures that the data importer must carry out (both sets of clauses suggest 17 categories of measures including requirements for pseudonymization and encryption, IT security governance and management, data avoidance and minimization, protection of data during transit and storage, and data quality);

*Data Subjects’ Notice and Enforcement Rights*

A provision in recital 11 of the European Commission’s “Implementing Decision on Standard Contractual Clauses for the Transfer of Personal Data to Third Countries Pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council” stating that “data subjects should be provided with a copy of the standard contractual clauses and be informed, in particular, of the categories of personal data processed, the right to obtain a copy of the standard contractual clauses, and any onward transfer.” The data exporter may redact business secrets and other confidential information, including the categories of technical and organizational measures described above, prior to providing copies of the third-country SCCs to data subjects. In addition, recital 12 of the implementing decision provides that data subjects may invoke and enforce the third-country SCCs against the data importer and data exporter;

*Data Breach Notices*

A provision requiring the data importer to notify both the data exporter and the competent supervisory authority in the event of a data breach;

*Compliance with Schrems II*

The addition of several provisions to comply with *Schrems II*. For example, the annex to the European Commission’s implementing decision on third-party SCCs includes a section titled “Local Laws and Obligations in Case of Access by Public Authorities” that provides the following:

- The parties warrant that they have no reason to believe the laws in a third country applicable to the data importer would “prevent the data importer from fulfilling its obligations under these [c]lauses.”
- The parties have conducted an assessment of “the specific circumstances of the
transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; [and] the storage location of the data transferred.”

- The parties have conducted an assessment of “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.”

- The parties have conducted an assessment of “any relevant contractual, technical or organisational safeguards [implemented] to supplement the safeguards” provided by the third-country SCCs.

- The data importer “has made its best efforts to provide the data exporter with relevant information” to conduct such assessments and “will continue to cooperate with the data exporter in ensuring compliance with [such assessments].”

- The parties have documented their assessments and will provide such documentation to the competent supervisory authority upon request.

- The data importer will promptly notify the data exporter if it becomes subject to laws or practices during the term of the third-country SCCs that prevent from it from fulfilling its obligations, including any changes in the laws of the third country.

- If the data exporter can no longer fulfill its obligations, “the data exporter [will] promptly identify appropriate [technical or organizational] measures” to correct the situation. If these measures cannot correct the situation, the data exporter will be entitled to terminate the third-country SCCs with the data importer.

- The data importer will promptly notify the data exporter and the data subject if it “receives a legally binding request from a public authority ... for the disclosure of [the] personal data transferred.” If the data importer is prohibited by law from notifying the data exporter or the data subject, the data importer will “use its best efforts to obtain a waiver of the prohibition” and communicate as much information as possible, as soon as possible. The data importer will also document its best efforts and make such documentation available to the data exporter upon request.

- The data importer will, at regular intervals during the term of the third-country SCCs, provide the data exporter with as much information as possible regarding the disclosure requests received, if the requests have been challenged, and the outcome of such challenges.

- The data importer will review the legality of the disclosure request and challenge the request if “there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity.” The data importer will pursue all possibilities of appeal regarding the legal
challenge. When challenging a disclosure request, the data importer will seek interim measures to suspend disclosure until the competent judicial authority has made a decision on the challenge. Further, “it [will] not disclose the personal data requested until required to do so under the applicable procedural rules.”

- The data importer will document its legal assessment and any challenge to the disclosure request and, if permitted by applicable law, make the documentation available to the data exporter and the competent supervisory authority upon request.

- “The data importer [will] provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.”

Recital 20 of the European Commission’s implementing decision regarding the third-country SCCs, and footnote 12 of the annex to the decision, provide that the parties, when conducting the risk assessment of the third country’s laws, may consider different elements “as part of an overall assessment, including reliable information on the application of the law in practice (such as case law and reports by independent oversight bodies), the existence or absence of requests in the same sector and, under strict conditions, the documented practical experience of the data exporter and/or data importer” and “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.” Thus, the European Commission has adopted a risk-based approach to the risk assessment.

**Key Takeaways**

Although employers currently using SCCs to transfer EU HR data to the United States and other third countries have 18 months to transition to the new controller-to-processor SCCs and third-country SCCs, they may want to consider beginning the transition process immediately because of the following:

- Many existing data processors and service providers may be unable or unwilling to comply with the requirements of these new SCCs, and employers may need to find new data processors and service providers that can and will comply with the new requirements.

- Employers and their data processors must conduct the risk assessments and implement the technical, contractual, and organizational supplementary measures required by Schrems II as part of the transition. These Schrems II requirements apply to all links in the data transfer chain, including onward transfers from the data processor to cloud providers and subcontractors. Employers and their data processors must also assess the laws of all third countries, including the United States, under which data may be transferred. Consequently, compliance with the Schrems II requirements will be time consuming and labor intensive.

- The Schrems II requirements do not apply just to the new SCCs; they immediately apply to current SCCs. Thus, to the extent that employers have not
complied with the Schrems II risk assessment requirements and supplementary measures obligations for their current SCCs, they may be in violation of Schrems II and subject to data protection authority enforcement actions and individual complaints. The Schrems II-compliant language in the European Commission’s implementing decision on third-country SCCs may serve as an example of provisions to include as addenda to existing SCCs in order to comply with Schrems II during the transition period.

- Employers may need to determine whether their transfers of EU HR data are controller-to-controller transfers, controller-to-processor transfers, processor-to-processor transfers, or processor-to-controller transfers and select the applicable modular language to create the appropriate clauses for each type of transfer.

In addition, employers may want to review the option to use multiple-party SCCs to consolidate the number SCCs they currently use.

After mid-September 2021, employers contemplating using SCCs for new data transfers must use the third-country SCCs for such transfers and conduct the required risk assessments and implementation of supplementary measures.

Employers may want to monitor the progress of the EDPB’s draft recommendations for complying with the Schrems II requirements that were issued on November 10, 2020, and are expected to be issued in final form in late June 2021. These recommendations set forth practical steps for conducting the risk assessment of third-country laws and practical advice for implementing the appropriate technical, contractual, and organizational supplementary measures to augment the protections provided by the new SCCs.

Employers that are also data processors or service providers for other employers may want to revise their business and data privacy practices to comply with the requirements of the controller-to-processor SCCs and third-country SCCs.


National Law Review, Volume XI, Number 165