New Data Transfer Mechanism Available for EU Personal Data

An analysis of the EU's new set of Standard Contractual Clauses by the data privacy and cybersecurity team at: Wilson Sonsini Goodrich & Rosati. Thanks to our good friend Cédric Burton for allowing us to share this.

New Set of SCCs for Data Transfers to Third Countries

On June 4, 2021, the European Commission (EC) published its long awaited new set of Standard Contractual Clauses (New SCCs). This new data transfer mechanism allows for the transfers of personal data outside of the European Economic Area (EEA) and replaces the current Standard Contractual Clauses (current SCCs). The New SCCs take into account the European Court of Justice's (CJEU) Schrems II ruling, which invalidated the EU-U.S. Privacy Shield and requires that data exporters and importers take measures to ensure that the SCCs are effectively complied with.

Importantly, the New SCCs allow for a risk-based approach to data transfer impact assessments when assessing the level of protection that will be provided to the transferred data. The New SCCs also try to address a number of concerns raised by the industry over the last decade, such as the need to cover more data transfer scenarios within the same set of clauses and to have more flexibility regarding the addition or withdrawal of parties to existing agreements.

Once published in the EC Official Journal, organizations will have a total of 18 months and 20 days to transition to the New SCCs. All organizations exporting or importing personal data subject to the General Data Protection Regulation (GDPR) will be impacted by the New SCCs. Companies should start assessing the impact of the New SCCS on their data processing practices, and should be planning an update of existing data processing agreements with vendors, customers, and intra-group agreements.

Overview

The New SCCs aim at modernizing the current SCCs in light of the significant developments in the digital economy, increasingly complex processing operations, and new requirements under the GDPR. They provide for enhanced flexibility for multi-party international data processing activities, while also setting forth specific safeguards and additional requirements in light of the case law of the CJEU, in particular the Schrems II ruling. (For the full story on the Schrems II decision, see our WSGR Data Advisor post *ECJ Invalidates EU-U.S. Privacy Shield and Upholds the Standard Contractual Clauses*).

A Modular Approach to Data Transfers

The New SCCs use a template framework that includes general clauses as well as modules that address different data transfer scenarios. Parties are able to select different versions of clauses to fit the relevant data transfer scenario. The New SCCs include four modules:

- *controller-to-controller (**C2C**),*
- *controller-to-processor (**C2P**),*
- *processor-to-controller (**P2C**) and,*
- *processor-to-processor (**P2P**) data exports.*

In practice, this means that the New SCCs are suited for data transfers not envisaged by the current SCCs, such as P2P and P2C transfers.

The New SCCs meet the requirements of Article 28 GDPR; thus, parties who enter into the New SCCs will no longer be required to also enter into a data protection agreement or addendum. In addition, the New SCCs can be included in a broader contract and supplemented with additional clauses as long as these do not contradict the New SCCs or otherwise prejudice the fundamental rights of data subjects.

Key Changes

The overall text of the New SCCs is more detailed than the current SCCs and introduces a high standard of accountability for both data importers and exporters. Because of the modular approach, obligations of parties will differ depending on the relevant data transfer scenario.

Selected examples of new clauses include:

- Docking clause. The New SCCs allow third parties to join the SCCs without the signature of all parties to the SCCs. The joining party only needs to complete the Appendix and sign the List of Parties annex.

- Onward transfer restrictions. The New SCCs only allow for the onward transfer of personal data by the data importer in specific circumstances, and the requirements differ depending on the data transfer scenario. For instance, in a controller-to-controller scenario, onward transfers are permitted if the third party i) becomes a party to the New SCCs or other binding instrument imposing the same level of data protection, ii) otherwise commits to appropriate safeguards (e.g., BCRs), iii) is based in a country that has been whitelisted by the EC, or iv) has signed an "onward data transfer agreement" with the data importer. Data may also be transferred based on the data subject's informed consent, or in limited other circumstances (e.g., the transfer is necessary to protect an individual's vital interests). If the importer is a processor, the New SCCs impose additional restrictions regarding subprocessing.

- Broad third-party beneficiary rights. The current and New SCCs are designed so that individuals can enforce the clauses against the exporter and the importer. This is important in particular for importers who will be subject to a range of new obligations under the New SCCs, with more direct liability than under the current SCCs. Also, important to note, is that not-for-profit organizations may initiate proceedings against importers or exporters on behalf of data subjects. To ensure individuals can enforce the clauses, the New SCCs must be governed by the

law of one of the EU Member States of the European Union that allows for third-party beneficiary rights.

- Broad transparency requirements. In C2C scenarios, data importers must provide notice regarding their data processing, including their identity, contact details, categories of data processed as well as any third party recipients of the data together with the purposes of the onward transfer and the ground(s) relied on. As this information will likely be provided through the exporter's privacy policy, we may see these policies becoming more detailed.

- Identification of the competent supervisory authority(ies). The parties will have to list their competent supervisory authority(ies) in an annex to the New SCCs. Where the data exporter is not established in the EU, but subject to the GDPR due to its targeting of individuals in the EU (either by offering good or services to these individuals or by monitoring their behavior), the competent supervisory authority will be the authority of the Member State where the data exporter has appointed a representative, or, in the absence of such representative, of the Member State where the targeted individuals are.

"Schrems II Provisions"

Further to the Schrems II ruling, the New SCCs contain a specific obligation on data exporters and importers to assess and ensure that the SCCs provide an adequate level of data protection in light of the legal regime of the destination country.

- Data transfer impact assessments. As in the current SCCs, parties must warrant that there is no reason to believe that the laws applicable to the data importer—in particular those relating to government access—will prevent the importer from fulfilling its obligations under the New SCCs. When doing so, parties may follow a risk-based approach and, for instance, take into account "documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests […]."[1] The New SCCs specify that the parties must document their assessment taking into account i) the specifics of the data transfer, ii) the laws and practices of the destination country (including those on government access), as well as iii) any additional safeguards the parties decide to apply to the transfer (such as contractual, technical, and organizational safeguards). If the importer becomes aware that it cannot fulfil its obligations, it must promptly notify the exporter, and the exporter must promptly identify and implement appropriate measures (such as technical or organizational measures). The exporter must suspend the transfer and is entitled to terminate the contract if there are no appropriate measures or if instructed to do so by the competent supervisory authority.

- Obligations in case of government access requests. Data importers must notify their data exporter(s) of any government access requests or when they become aware of any direct government access. If legally prohibited from doing so, the importer should use its best efforts to obtain a waiver of the prohibition. The New SCCs also require that importers update exporters "at regular intervals" with as much relevant information as possible on requests received and keep such information on file for supervisory authorities. Furthermore, data importers are required to i) review the legality of the government access request, ii) review whether there are grounds to challenge the requests, and iii) if so, to exhaust all available remedies to do so. All such steps should be documented and made available to the exporter and competent supervisory authority upon request. In practice, this means that data importers will need to set up procedures to ensure adequate compliance with these requirements in case of government access requests.

Timing

Organizations can continue to conclude the current SCCs for three months and 20 days after the publication of the New SCCs in the EC Official Journal. After this date, organizations will have 15 months to transition to the new SCCs, while continuing to rely on the current SCCs, provided that the underlying processing activities remain unchanged. In the event of changes, the parties will need to replace their current SCCs with the New SCCs. Thus, organizations have a time period of 18 months in total to transition from the old SCCs to the New SCCs. While an 18-month transition period seems manageable, organizations with many vendors, customers, and partners should consider beginning their implementation efforts now.

Next Steps

As explained above, the New SCCs impose a range of new obligations. All organizations exporting or importing personal data subject to the GDPR will be impacted by the New SCCs. Companies should carefully review the New SCCs and assess their impact on their organization. In particular, they should start planning an update of existing data processing agreements with vendors, customers, and intra-group agreements. In addition, data importers that are not directly subject to the GDPR may have to set up a compliance program to meet the New SCCs' requirements.

June 4, 2021

[1] *See Clause 14, footnote 12 to the New SCCs.*

Wilson Sonsini Goodrich & Rosati routinely advises clients on GDPR compliance issues, and helps clients manage risks related to the enforcement of global and European data protection laws. For more information, contact ***Cédric Burton***, ***Jan Dhont***, ***Lydia Parnes***, ***Christopher Olsen***, *or another member of the firm's* ***privacy and cybersecurity*** *practice. Laura Brodahl, Carol Evrard, Joanna Juzak, and Sam Meijer contributed to the preparation of this alert.*