WILSON SONSINI

European Commission Issues New SCCs for Data Transfers to Third Countries

CONTRIBUTORS

Christopher N. Olsen

Cédric Burton

ALERTS

November 17, 2020

On November 12, 2020, the European Commission (EC) issued a draft version of a new set of Standard Contractual Clauses (New SCCs). The long-awaited New SCCs include several modules that companies can use depending on the transfer scenarios, such as controller-to-controller, controller-to-processor, and processor-to-processor data exports. The New SCCs have also been updated to reflect the high standard for data protection set forth in the General Data Protection Regulation (GDPR) and to take into account the requirements resulting from the *Schrems II* ruling.

The New SCCs are subject to public consultation until December 10, 2020, and they will be reviewed by the European Data Protection Board (EDPB) and European Data Protection Supervisor (EDPS). Once the final version of the New SCCs is issued, organizations will have a one-year transition period to implement them. During that time, the current SCCs will stay in effect. Nonetheless, organizations should consider preparing for the New SCCs and strategize on how to use the New SCCs for current and future data exports.

This alert summarizes the most important changes. For a deeper dive on this topic, please register here for our EU privacy and cybersecurity team's webinar on Thursday, November 19, 2020, at 9 a.m. PT/12 p.m. ET/6 p.m. CET. For more information on the EDPB's recommendations, please see our post on The WSGR Data Advisor, "EDPB Publishes Draft Recommendations on Supplementary Measures for Data Transfers."

Background

Stakeholders have been anticipating the New SCCs for a long time. The current SCCs were adopted in 2001, 2004, and 2010 under the pre-GDPR Data Protection Directive (1995/46) and have been criticized for providing insufficient flexibility in an increasingly complex and international data processing reality. The SCCs were due to be revised in light of the GDPR. The *Schrems II* ruling accelerated this process, because the SCCs offer businesses a practical alternative to the Privacy Shield, which is now invalidated (read about the *Schrems II* decision in 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 adopt a one-size-fits-all approach and can be used for varying transfer scenarios. This is accomplished through a modular approach whereby parties may select different versions of clauses to fit the relevant data transfer. This means that the New SCCs should be suitable for data transfers previously not envisaged by the SCCs, such as processor-to-processor and processor-to-controller transfers. The New SCCs meet the requirements of Article 28 GDPR, which means that parties who have entered into the New SCCs will no longer need a data protection agreement or

Copyright © 2024 Wilson Sonsini Goodrich & Rosati. All Rights Reserved.

addendum alongside the SCCs. The New SCCs can be made part of a broader contract and supplemented with additional clauses, as long as these do not contradict the New SCCs or prejudice the fundamental rights of data subjects.

Key Changes

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

Select examples of new clauses include:

- **Stricter onward transfer restrictions.** The New SCCs allow for the onward transfer of personal data by the data importer only in a specific number of cases, such as, for instance, if the third party: i) becomes a party to the SCCs; ii) commits to appropriate safeguards (e.g., BCRs); iii) is based in a country that has been whitelisted by the European Commission; or iv) has signed up to an "onward data transfer agreement" with the data importer. Data may also be transferred based on the data subject's informed consent.
- **Broad third-party beneficiary rights.** Data subjects are granted third-party beneficiary rights that are generally broader than under the previous sets of SCCs. For instance, such rights can be enforced both against the data exporter and data importer.
- **Broad transparency requirements.** In controller-to-controller scenarios, data importers must provide notice regarding their data processing, including their identity, contact details, new processing purposes, and any third-party recipients of the data. This information will most likely be provided through the exporter's privacy policy, which will likely mean that privacy policies will become more detailed on these points.

"*Schrems II* Provisions"

Further to the *Schrems II* ruling, the New SCCs contain specific obligations for the data exporters and importers to assess that the SCCs can provide an adequate level of data protection in light of the legal regime of the country/countries of data import.

- **Organizations must evaluate the laws of the third country.** As in the previous SCCs, the parties must warrant that there is no reason to believe that the laws applicable to the data importer, in particular those relating to disclosure of personal data to public authorities, will prevent the importer from fulfilling its obligations under the New SCCs. However, the new SCCs are more specific on these obligations. Mirroring the EDPB's recent recommendations and the *Schrems II* ruling, the parties must declare they have taken into account the specifics of the data transfer and the laws of the destination country, as well as any additional safeguards the parties decide to apply to the transfer. The importer must provide the exporter with relevant information on these points and continue to cooperate with the exporter to ensure compliance. If the importer becomes aware that it cannot fulfill 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 then notify the competent DPA if it intends to continue the transfer on the basis of such additional measures. Otherwise, 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 DPA.
- **Obligations in case of government access requests.** Data importers will be required to notify the data exporter(s) upon receiving government access requests or upon becoming aware of any direct government access data transferred. If legally prohibited from doing so, the importer should use its best efforts to obtain a waiver of the prohibition. The New SCCs also stipulate that data importers "regularly" update exporters on requests received and keep such information on file for DPAs. Furthermore, data importers would be 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, exhaust all available remedies to do so. All such steps should be documented and made available to the exporter and competent DPA upon request.

What Should Companies Do?

Interested parties can submit comments on the New SCCs until December 10, 2020. The current SCCs will be repealed once the New SCCs are finalized, which is expected to be in early 2021 at the earliest. Organizations will have a one-year transition period to bring all their data transfers in order under the New SCCs. During the transition period, companies may continue relying on the existing SCCs, although they should supplement such SCCs as necessary to ensure a sufficient level of protection under the GDPR. During the lead-up to implementation, organizations should start familiarizing

Copyright © 2024 Wilson Sonsini Goodrich & Rosati. All Rights Reserved.

themselves with the New SCCs to prepare for the transition, and they should review the EDPB's recommendations in parallel, as the recommendations will apply to the New SCCs.

Our EU privacy and cybersecurity team is closely monitoring this topic and will provide updates when they are released.

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, please contact Cédric Burton, Jan Dhont, Lydia Parnes, Christopher Olsen, or another member of the firm's privacy and cybersecurity practice.

Lore Leitner, Alexandre Lépine, and Christopher Foo contributed to the preparation of this alert.

Copyright © 2024 Wilson Sonsini Goodrich & Rosati. All Rights Reserved.