EU Issues New Standard Contractual Clauses for Data Transfers

June 21, 2021

The European Union limits the transfer of EU personal data to countries whose privacy regimens are not deemed "adequate," like the United States. American companies have tended to rely upon Standard Contractual Clauses (SCC) for such transfers out of the EU. Last summer, the European Court of Justice invalidated the Privacy Shield data transfer mechanism. In that same "*Schrems II*" opinion, the Court questioned whether SCCs (last amended in 2004) provide sufficient data protections.

In response to this uncertainty, the European Commission recently adopted new Standard Contractual Clauses (SCC) that become effective June 27, 2021. The new SCCs should increase the confidence of American businesses in the GDPR-compliant transfer of personal data of EU residents to servers in the U.S., provided those businesses know when and how to use them.

What are Standard Contractual Clauses?

The European Commission publishes the SCCs as model provisions contracting parties can adopt, typically as addenda to data processing agreements, to effectuate EU personal data transfers to "inadequate" countries. The parties cannot generally modify the SCCs.

SCCs provide for EU regulatory jurisdiction over the parties with respect to the EU personal data transferred. They impose certain security and privacy obligations on the parties. EU residents may enforce their privacy rights against the importer or exporter of the personal data.

The SCCs and the GDPR classify parties as either "controllers" or "processors." Controllers determine the purposes and means of the processing of personal data. Processors process personal data upon the instructions of the controller.

What's New in the New SCCs?

The new SCC's cover four transfer scenarios or "modules": Controller-to-Controller, Controller-to-Processor, Processor-to-Processor, and Processor-to-Controller. To address concerns expressed in *Schrems II*, companies must assess the risk of non-EU governments accessing the data. For example, if an American company determines that it is unlikely that the U.S. will seek the EU personal data under Section 702 of the

FISA Act, it may utilize the SCCs. Other new and newsworthy items in the SCCs include:

- **Application to Non-EU Data Exporters**: The exporter of EU personal data may be outside the EU.
- **Multi-party SCCs**: Multiple parties may enter into the new SCCs.
- **No Separate DPA Always Required**: In the case of controller-to-processor and processor-to-processor transfers, no additional data processing agreement is needed.
- **Baked-In Liability**: Clause 12 of the new SCCs state that each party shall be liable to the others for damages it causes them by breaching the SCC. It is not yet clear whether parties may shift such liabilities by contract.
- **Data Subjects May Request SCCs**: Upon request, a party must provide a copy of the SCC to an individual whose data is being processed, but it can redact business secrets and other confidential information.
- **Data Transfer Impact Assessment**: Parties must perform and document a data transfer impact assessment (DPIA) and make it available to the competent supervisory authority upon request.
- **Government Access:** A data importer must challenge government access requests if reasonable grounds exist and make its legal assessment available to the data exporter (and the competent supervisory authority) upon request.
- **Security Measures:** Annex II to the new SCCs lists the technical and organizational security measures necessary to ensure an appropriate level of protection.
- **Extended Transition Period**: Parties can adopt the existing SCCs until September 27, 2021 but must transition to the new SCCs by December 22, 2022.

The new SCCs should prompt an 18-month endeavor by U.S. businesses to evaluate their data flows and transfer mechanisms, including to and from the cloud. It should incorporate DPIAs into the evaluation process, and document the likelihood of and anticipated response to government requests for EU personal data.

Noncompliance with the GDPR's cross-border data transfer restrictions could potentially trigger fines of up to 4% of annual revenues. Our Global Privacy, Cybersecurity and Data Protection practice can help your business address the strategic, legal, and logistical issues in using these new SCCs.

For more information, please contact Tedrick Housh, Michael Cohen, or your regular Lathrop GPM attorney.