DAVIS GILBERT

Digital Media, Technology + Privacy

European Commission Adopts Revisions to Standard Contractual Clauses

The Bottom Line

- The revised SCCs published by the European Commission will provide businesses with more flexibility to enter data sharing arrangements with controllers and processors outside of the European Economic Area.
- Businesses should revisit their contractual arrangements and identify any agreements that incorporate the prior versions of the SCCs. The Commission has given businesses 18 months, starting from June 27, 2021, to update all contracts incorporating SCCs for data transfers outside the EEA.

The European Commission (Commission) issued updated Standard Contractual Clauses (SCCs) on June 4, 2021. The long-awaited announcement follows a 2020 decision by the EU's highest court to overturn the EU-US Privacy Shield Framework (Privacy Shield), which previously allowed for data transfers between the European Union and the United States (see our prior Alert). The publication of the revised SCCs will help global businesses comply with the European General Data Protection Regulation (GDPR) when transferring personal data to affiliates and third parties outside of the European Economic Area (EEA).

The Importance of Standard Contractual Clauses

Under the GDPR, transfers of personal data to any country outside the EEA may take place if the recipient country ensures an adequate level of protection for data as determined by the Commission. Until last year, companies transferring data from the EEA to the United States were able to rely on the Commission's position that U.S. companies registered with the Privacy Shield program were deemed adequate. However, in July 2020, the Court of Justice of the European Union (CJEU) invalidated the Privacy Shield as part of its "Schrems II" decision, forcing businesses to consider other legal mechanisms for cross-border data transfers.

In the absence of an adequacy decision, the GDPR requires that companies implement appropriate safeguards, including

enforceable data subject rights and legal remedies. The most frequently used mechanism has been the SCCs – a contract pre-approved by the Commission that establishes certain controls to safeguard data as per EU standards.

Notably, the Schrems II decision upheld SCCs as a valid transfer mechanism in the aftermath of Privacy Shield, but required that EU companies have additional supplemental measures in place based on the laws, standards, and practices in the jurisdiction where the data is to be transferred. Such measures, even those recommended by the European Data Protection Board (EDPB), were often ad hoc and unpredictable.

Revisions to the SCCs were sorely needed in light of the Schrems II decision, and the newly-published language is heavily influenced by the CJEU's ruling. Moreover, the previous SCCs pre-dated the GDPR and needed to be updated to fit the current legal framework, regardless of the recent judicial developments.

Key Changes to the Standard Contractual Clauses

- **One Integrated Document:** Companies looking to adopt SCCs were previously forced to choose between three variants – two for controller-to-controller transfers (approved by the Commission in 2001 and 2004), and one for controller-to-processor transfers (approved in 2010). The new SCCs come in the form of a single, holistic agreement, rather than separate documents.
- **Modular Design:** The revised SCCs employ a modular approach where general clauses can be combined with specific clauses unique to controller-to-controller, controller-to-processor, processor-to-processor, and processor-to-controller data transfers. This allows companies some flexibility to tailor the contractual language to their business needs.
- **Multi-Party Transfers:** While the previous SCCs were drafted for data transfers between two parties, the new version has a "docking clause" that allows additional parties to opt in. SCCs can now be used for onward transfers to parties further down the data processing chain, and those new parties can be added over time, so long as they agree to be bound by the SCCs.
- **Required Security Measures**: Parties to the new SCCs are required, under Annex II, to describe technical and organizational security measures "in specific (and not generic) terms." This requirement is not limited to the data importer – it also applies to any subsequent processors or sub-processors.

- **Establishment No Longer Required:** While the language of the previous SCCs required data exporters to be established in the EU, the revised terms explicitly recognize that data exporters can be non-EU entities. This change is useful for companies that are established outside of the EU but still subject to the GDPR by virtue of the extraterritorial scope in Article 3(2).

- **Mandated Focus on Local Laws and Practices:** In an attempt to satisfy the CJEU's Schrems II ruling, the new SCCs require the data exporter and importer to "warrant that they have no reason to believe that the laws and practices in the" recipient country "prevent the data importer from fulfilling its obligations under" the SCCs.

  Such warranties must be based on a documented assessment taking into account:

  1. The specific circumstances of the data transfer;
  2. The laws and practices of the destination country (including such laws authorizing access by or requiring disclosure of data to public authorities); and
  3. Any relevant contractual, technical or organizational controls in place to supplement the safeguards under the SCCs.

  Importantly, the SCCs note that such assessments "may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests."

- **Obligations Concerning Legally Binding Requests for Data:** In the same vein as the above requirements as they relate to Schrems II, the revised SCCs require a data importer to notify the data exporter and (where possible) the data subject if it:

  1. "Receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred"; or
  2. "Becomes aware of any direct access by public authorities to personal data transferred."

  The data importer is also required to review and challenge the legality of the disclosure, and use its best efforts to obtain a waiver from any legal prohibition on notifying the data exporter or data subject of the disclosure.

For More Information

Please contact the attorneys listed below or the Davis+Gilbert attorney with whom you have regular contact.

Gary A. Kibel

Partner
212 468 4918
gkibel@dglaw.com

Oriyan Gitig

Counsel
212 468 4880
ogitig@dglaw.com

Zachary N. Klein

Associate
212 237 1495
zklein@dglaw.com