Transferring Personal Data

Importance of Standard Contractual Clauses

Ryan Sulkin, Michael Stovsky, Jonathan Todd, Kristopher Chandler
Benesch, Friedlander, Coplan & Aronoff LLP


Kristopher J. Chandler


Michael D. Stovsky


Ryan T. Sulkin


Jonathan R. Todd

The European Commission's long-awaited updates to the Standard Contractual Clauses ("SCCs") have arrived. Data protection lawyers globally have anticipated these changes, which are necessary to address a legal landscape remade by the GDPR and, more recently, the Schrems II decision. Those in the transportation space should be hyper aware of these changes as they may impact current and future activities.

What are the Key Deadlines?

The new SCCs will become effective twenty (20) days following their publication in the Offcial Journal of the European Union (placing the anticipated effective date in the end of June or early July timeframe). The new SCCs are eligible for use immediately after their effective date. With respect to the old SCCs, there are two (2) key dates to keep in mind.

- The old SCCs can only be newly signed for a period of three months after the new SCCs come into effect. Thereafter, only the new SCCs can be newly signed.
- Versions of the old SCCs signed prior to the cut-off date noted above are considered "grandfathered in" and are therefore deemed valid for an additional period of 15 months following the cut-off date provided that:
- The processing described under the old SCCs has not changed; and the reliance the old SCCs ensures that the transfer of personal data is subject to appropriate safeguards (which means in practice that the risk assessment required by Schrems II will need to be completed).

Bottom line, all old SCCs will need to be replaced within approximately 18 months.

What is the purpose of the SCCs?

Taking a step back, the historical purpose of the SCCs (as carried forward under the GDPR), was to allow for the transfers of personal data from geographic locations within the European Economia Area (EEA) to geographic locations outside of the EEA deemed not to have adequate data protection law. The United States is one of many countries deemed to have inadequate data protection law by the EU. Use of SCCs has grown significantly in recent years as a result of the instability of the EU-US Privacy Shield program and its predecessor, the EU-US Safe Harbor program.

How have the SCCs changed?

The new SCCs come in two different sets.

The first set of SCCs addresses the traditional paradigm, transfers of personal data from geographic locations within the EEA to geographic location outside of the EEA. However, unlike the old SCCs which only offered controller to controller and controller to processor versions, this first set of new SCCs offers two additional options (four options in total) as follows: (i) controller to controller; (ii) controller to processor; (iii) processor to processor; and www(iv) processor to controller, covering data sharing paradigms that the old SCCs struggled to address with clarity. The second set of new SCCs, which did not exist in a prior form, covers the engagement of data processors in the EEA when a cross-border data transfer outside of the EEA is not involved and satisfies the requirements for engaging processors under Article 28 of the GDPR.

What about the Schrems II decision?

The first set of new SCCs contain contractual provisions designed to address the concerns raised by the Schrems II decision, including specific obligations when there is a government request for personal data in a non-EEA destination country. For example, the data importer is required to challenge government access requests if there are reasonable grounds for doing so and pursue possibilities of appeal where reasonable. The data importer must document its legal assessments in this respect and make them available to the data exporter and the competent supervisory authority upon request. The new SCCs also require the signing entities to conduct and document a data transfer impact assessment and make it available to the competent supervisory authority upon request. When undertaking their data transfer impact assessment, the parties may consider "relevant and documented practical experience with prior instances of request for disclosure from public authorities, or the absence of such requests." In addition, further guidance from EU regulators may require additional contractual or operational protections beyond language currently in the new SCCs. Accordingly, this is an area that must be monitored closely.

Additional Interesting Details

- The new SCCs permit a data exporter to be established outside the EU, aligning with the extra-territorial reach of the GDPR.

The new SCCs also enable multiple parties to enter into the SCCs, aligning with how many organizations currently address intra-group data transfers (essentially, versions of the SCCs entered into by relevant company affliates to address EEA to non-EEA personal data transfers.)

The new SCCs state: "each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses." As a result, it remains an open question as to whether the SCCs will allow one party to limit their liability to the other party by adding bolt-on language to the SCCs, which is currently a common practice.

Annex II of the new SCCs requires more specific detail with respect to security measures in place and offers more specific suggestions for these measures.

Currently, the new SCCs are not required for transfers of personal data from within the UK to outside of the UK; however, a similar SCC construct will likely be required by the UK in the future. It is also currently undecided as to whether the European Commission will require SCCs for personal data transfers from the EEA to the UK (or whether the UK will be deemed "adequate" such that SCCs are not required.)

> The US is one of many countries deemed to have inadequate EU data protection law. Use of SCCs has grown significantly in recent years as a result of the instability of the EU-US Privacy Shield program and its predecessor, the EU-US Safe Harbor program.

Impact on Transportation

Players in the transportation space need to be keenly aware of how their enterprise utilizes, discloses, and transfers information containing personal data governed by the GDPR to ensure that compliance objectives are met. When engaging with foreign service providers that process personal data on their behalf, organizations may need to adopt these SCCs when required by business activities.

Certain data security and privacy obligations, including the obligating to adopt the SCCs are implicated in a number of transportation contexts. When participating in a document exchange with service providers, personal data may be exchanged between the parties. This exchange may trigger GDPR compliance obligations. When collecting origin and destination information for a particular shipment, this collection may trigger GDPR compliance obligations. When finalizing internal shipments, these operational activities may trigger GDPR compliance obligations. As such, enterprises that even tangentially touch the European Union will need to ensure that they understand how they collect, use, disclose, and transfer personal data by conducting comprehensive data mapping exercises to mitigate any liability exposure.

A robust data mapping exercise is a key first step to understanding how to adopt these SCCs.

It is important to note that data and security and privacy compliance obligations are also ever present in the B2B space as activities not involving consumers may still involve the transfer of personal data. A keen awareness of an enterprise's collection of personal data, even outside of interactions with consumers, is necessary to avoid regulatory pitfalls.

Takeaways

Now that the new SCCs are a known commodity, it is time for organizations to design and begin implementation of a comprehensive strategy for replacement of existing SCCs, both with third parties and between their own affliates in the intragroup personal data transfer context. In addition, enhanced procedural and documentation requirements within the new SCCs mean that signing the SCCs will be much more than an exercise on paper, making the need to prepare early all that more important. The Data Protection team at Benesch is available to answer any questions that you may have and support your organization with its transition to the new SCCs.

About the Authors

Kristopher J. Chandler- Kris focuses his practice on complex corporate and technology transactions, intellectual property protection, data security and privacy, regulatory guidance, corporate and regulatory assistance in the transportation industry.

As an intellectual property lawyer by trade, Kris represents clients in various sophisticated technology transactions, assisting high-tech companies to market, protect, commercialize, and distribute their intellectual property. In addition, Kris has experience navigating the various data security and privacy regulations of the United States, including HIPAA, as well as those in Canada and Europe, including the General Data Protection Regulation. Kris has represented numerous clients, with domestic and international business operations, in developing and implementing compliant data security and privacy policies and procedures.

Michael D. Stovsky- Mike leads Benesch's Innovations, Information Technology & Intellectual Property (3iP), Technology Deals, Data Security and Privacy, and Blockchain and Smart Contracts practices. He also serves as Benesch's EU GDPR Data Protection Officer and is a member of the Executive Committee.

Mike has nearly three decades of experience representing technology companies from start-up to Fortune 100, as well as major regional and national venture capital and private equity funds and their portfolio companies, as lead outside technology transactions, IP, and privacy/data security counsel. He helps companies negotiate, close, and handle complex, high-value, IP and technology transactions.

Ryan T. Sulkin- Ryan is a partner and the Data Protection Group Lead in Benesch's 3iP Practice Group. Ryan's practice resides squarely at the intersection of technology and data.

Ryan regularly advises clients with respect to complex technology transactions, including SaaS, cloud, software development, professional services, and outsourcing arrangements. He also provides risk-based and actionable legal counsel to clients on data privacy and cybersecurity matters across a wide range of data-rich, highly regulated industries, including financial services, payments, health care, higher education, retail, hospitality, and technology. He regularly advises clients with respect to CCPA, CPRA (and similar laws emerging in numerous US states), GDPR, HIPAA, GLBA, TCPA, FCRA, COPPA, CAN-SPAM, PCI-DSS, NYDFS, data breach notice laws, and cross-border matters involving global laws and regulations.

Jonathan R. Todd- Jonathan's practice targets the risks and opportunities that businesses encounter when goods move through domestic and international supply chains.

All providers and users of supply chain services face challenges in transportation and logistics, warehousing and distribution, customs and trade, procurement and business operations, as well as the disputes that follow. He represents manufacturers, distributors, retailers, carriers, brokers, and forwarders that contribute at every step of the end-to-end supply chain in those matters. Their objectives often require business consult, regulatory compliance counseling, mergers and acquisitions strategy, drafting and negotiation of contracts, litigation and dispute resolution, and enforcement defense including during investigations and audits.

About Benesch Law:

Benesch is an AmLaw 200 business law firm and limited liability partnership with offices in Chicago, Cleveland, Columbus, Hackensack, San Francisco, Shanghai and Wilmington. The firm is known for providing highly sophisticated legal services to national and international clients that include public and private, middle market and emerging companies, as well as private equity funds, entrepreneurs, and not-for-profit organizations.

NOTE: For information, please visit: https://www.beneschlaw.com