Standardizing data-processing agreements globally

Sep 28, 2021

Privacy professionals around the world are feverishly working on configuring and implementing the European Union's new standard contractual clauses. Effective Sept. 27, companies in the European Economic Area entering into new cross-border data transfer arrangements with companies outside the EEA based on SCCs must adopt the new versions. Any recipient that signs the new SCCs promises it has matching agreements in place with its own vendors according to Clauses 8.8 and 9. Myriad businesses are affected because every company has numerous affiliated and unaffiliated vendors and other business partners worldwide. To remain open to businesses from the EEA, all companies need to have the new SCCs in place by Sept. 27.

To further complicate an already difficult situation, many countries have issued requirements that businesses must impose similar and different contractual clauses to protect the personal data of their residents, including, most recently, several U.S. states. Additionally, businesses have to flow these other clauses through to multiple tiers of service providers. Addressing these requirements with separate contracts, one country at a time, becomes quickly unmanageable. A medium-size multinational business with subsidiaries, employees and customers in 20 jurisdictions and vendors in an additional 20 jurisdictions would need to implement 400 data transfer and processing agreements. If each of those vendors has 20 vendors, we are counting 8,000 contracts originating from one multinational business, and that is before we have looked at additional tiers of suppliers and considered that large businesses have thousands of vendors.

Privacy professionals need to develop practical approaches. Companies need to work collaboratively with supply chains and customers to pursue solutions that all businesses can scale globally. In-house counsel cannot afford to focus just on the new SCCs. Multistakeholder compliance teams within companies need to address requirements for data from multiple jurisdictions at the same time. For most service providers, this is not only a compliance topic, but also an urgent condition to sales and commercial success.

Implementing the new SCCs

Just dealing with the latest from the old world presents challenging problems: The new SCCs consist of more than 25 pages — the word count exceeds 11,400 — contain multiple modules, mandate selections, and require companies to fill out annexes and prepare detailed written descriptions of security measures, processing instructions and cross-border transfer impact assessments.

Companies must adopt the clauses without revisions or modifications to enjoy the corresponding exceptions under the EU General Data Protection Regulation, according to Clause 2. Companies are not prohibited from adding commercial clauses concerning liability, warranties, disclaimers and indemnification but must not contract Clause 12, e.g., by completely rendering the clauses ineffective by way of an absolute limitation of liability. But, in practice, it is preferable to address risk allocations in separate commercial agreements, to avoid complicating or delaying the implementation of the new SCCs, in which both parties have a common interest. In many cases, the commercial agreements are already in place or being negotiated by separate teams of attorneys and procurement professionals who privacy professionals may prefer not to draw into intricacies of data-processing agreements.

Multiple modules may apply to any given business relationship. Therefore, companies should consider adopting the new SCCs in their entirety and defining their applicability to particular data transfers in Annex 1 instead of signing up to individual modules separately.

Multinational companies that insist on separate, direct bilateral contracts between every subsidiary and subprocessor on the vendor side are demanding the impractical. In most situations, solutions have to include hub-and-spoke contracting models in which one entity in the customer group engages with one entity in the vendor group and then they pass the contractual commitments to their respective affiliates. Incorporation by reference and multiple parties signing one contract should also be considered. To help each other, the parties could agree to sign separate, additional bilateral versions in case of a legitimate need.

Businesses should also think long and hard about the pros and cons of using the new SCCs for processing arrangements within the EU. These are shorter and less burdensome but introduce extra complexities. Alternatively, companies can use the new SCCs across the board for processing agreements within the EU, given the European Commission expressly stated the new SCCs, "should also allow to fulfil the requirements of Article 28(3) and (4)" of the GDPR and constitute "standard contractual clauses pursuant to Article 28(7)" of the GDPR, see Clause 2 and Recitals 8 and 9 of Commission Decision (EU) 2021/914 of June 4, 2021.

With the new SCCs, companies have to agree on instructions for processors, which can refer to the service provider's standard technical specifications. Also, companies need to document "transfer impact assessments" pursuant to Clause 14, implementing requirements that the Court of Justice of the European Union promulgated in its "Schrems II" decision and the EDPB expanded in its final recommendations June 18. Several German data protection authorities have started to audit German companies with questionnaires, asking questions such as, "If you have concluded that the recipient can in fact guarantee compliance with the contractual obligations under the SCCs, please describe in detail your reasons for this conclusion and provide appropriate evidence." Service providers outside the EEA should proactively prepare information for such assessments to render their offerings legally usable for customers in the EEA.

Divided state laws in the US

Multiple states have passed omnibus privacy laws, inspired by the California Consumer Privacy Act, as amended by the California Privacy Rights Act. Companies doing business in or with the U.S. must deal with this patchwork of laws until possible harmonization comes from an omnibus federal privacy law. On the customer and vendor side, companies need to consider their position with respect to "selling personal information." They cannot rely on exceptions for processing arrangements unless they agree on particular terms relating to selling and sharing for cross context-behavioral advertising and personal information are put in place. Slightly different terms are required for all controller-to-processor flows of personal information under Virginia's Consumer Data Protection Act and the Colorado Privacy Act. Seemingly simple clauses, like "vendor agrees to comply with California privacy laws," are ineffective and insufficient because customers need statutorily prescribed commitments concerning the use and sharing of the customer's data.

Some companies have started to integrate legally mandated data-processing terms into commercial agreements. Others have created detailed, state-by-state addenda with complicated and repetitive terms. Form agreements often conflate commercial questions, such as risk allocation, with compliance questions, the legal need to put certain contractual terms in place, and lead to lengthy negotiations and documentation that cannot easily be leveraged for new contracts. To avoid the adverse impact on sales

cycles and legal budgets, companies should consider consolidating mandated clauses in a concise set of data protection standards they would be willing to agree to as customers or service providers — which most companies are in different parts of their businesses.

Most requirements can be addressed on less than two pages with pragmatic and concise drafting. At the end of the day, processors must commit to using the customer's personal data only to provide their service and keep the data secure. If one adds a few more statutorily required concepts, one can address 80% to 90% of requirements in data protection laws around the world. Keeping the document as short as possible means fewer words for all involved to review and negotiate. And adding terms that are legally necessary for the data-processing agreement should greatly reduce the need for negotiations. What it should come down to between the parties is an alignment on the roles of the parties, controllers-to-businesses or processors-to-service providers, and the rest should follow.

Beginning Jan. 1, 2023, the CCPA includes a third possible characterization of a "contractor" that imposes fewer limitations on processing activities compared to those applicable to a "service provider." But the contractor characterization is more challenging to align with a processor characterization under the Virginia and Colorado laws and the GDPR and, therefore, a less practical option. To the extent it applies, the U.S. Health Insurance Portability and Accountability Act warrants its own separate "business associate agreement" but should also be kept separate from the commercial agreement and only cover the legally required terms.

Latin America

Countries in Latin America have not yet harmonized their data protection laws or developed a uniform approach to cross-border data transfers.

Argentina and Uruguay have qualified for "adequacy" decisions by the EU Commission. This means companies in the EEA can transfer personal data to these countries without signing the new SCCs or conducting detailed transfer impact assessments. Yet, companies might want to rely on them anyway in the interest of standardization because customized agreements as an alternative create additional burdens on contracting processes.

For transfers of personal data from Argentina, the Agency of Access to Public Information has published its own model clauses for international data transfers to countries not deemed adequate by the DPA. It might also accept the new SCCs instead of its own model clauses, given that it accepted the earlier versions. The same approach should be viable for Uruguay. Companies that follow this approach should be clear in their contracts that they apply the new SCCs also to personal data concerning data subjects in Argentina and Uruguay. This expansion in scope seems suitable for countries with GDPR-like laws, in the interest of standardization, but should be avoided for countries with entirely different regimes, particularly those with significant risks of private litigation, like the U.S.

Other countries in Latin America have had data privacy laws in place for a while and requirements for international data transfers without reference to model clauses, such as Colombia and Mexico. In Mexico, international data transfers must be consented to by data subjects in the relevant privacy policy, an intra-group transfer necessary for the performance of a contract with the data subject, compliance with a legal obligation, the enforcement of rights or public interest. In Colombia, international data transfers are prohibited unless to a country deemed an adequate jurisdiction by the Superintendencia de Industria y Comercio, the data subject grants express consent, the transfer is necessary for the performance of a contract with the data subject or the transfer serves public interests. Under Colombian law, when the transfer takes place between a controller and processor or between two processors that follow the same privacy policy, it is a data transfer, controller-to-controller, or

transmission, controller-to-processor. All data transfers and transmissions in Colombia must be documented in a data-sharing agreement.

Other countries in the region, such as Chile, do not have a comprehensive data protection law yet so there are no specific requirements for using SCCs. Yet, other countries that are not deemed adequate jurisdictions by the EU Commission have data protection laws in place and will accept that international data transfers rely on the EU Commission–approved SCCs. In Peru, international data transfers under Peruvian law are authorized if they are supported by a written agreement that will guarantee the same level of protection as Peruvian law and, for that purpose, the old and new EU SCCs are acceptable. In addition to a written agreement, under Peruvian law, data subjects must grant express consent to international data transfers except if necessary for performing a contract with the data subject or in case of public interest.

Last but certainly not least, Brazil has enacted a General Data Protection Law that entered into force in September 2020 and is similar to the GDPR. One of the transfer mechanisms under the law is model clauses, but Brazil's Autoridade Nacional de Proteção de Dados has not yet published any. Although there is no official statement from the DPA in that regard, considering the law in Brazil was inspired by and followed the same principles as the GDPR, many businesses expect the new SCCs will be deemed acceptable for personal data transfers from Brazil, as well.

Asia-Pacific

Countries in the Asia-Pacific region have not made any real attempts at harmonizing their national privacy laws on a regional basis. Countries that have enacted privacy laws will find them quite different from their neighbors' laws. But they have been working on solutions for cross-border data transfers, including within the Asia-Pacific Economic Cooperation framework.

Some APAC countries have not yet enacted specific privacy or data protection laws with explicit, omnibus cross-border transfer restrictions, including Vietnam, Indonesia and Thailand. Thailand's laws have been drafted and are based loosely upon the GDPR; they will come into force next year.

Countries with moderately long-standing privacy laws, such as Australia, New Zealand, Singapore, the Philippines and Malaysia, increasingly align their laws to the GDPR. In many of these jurisdictions, some form of contractual requirement may be required and acceptable to ensure the legitimate transfer of personal data outside their jurisdictions. Most APAC countries have not prescribed national SCCs or expressly endorsed the EU's SCCs. Singapore's Personal Data Protection Commission has acknowledged the EU SCCs may be adopted, but other countries have remained silent on this point. Therefore, companies have to carefully consider the pros and cons of expanding the scope of the new SCCs to personal data from these jurisdictions. Many are likely to hold off until clearer needs and benefits emerge and, in the meantime, use more focused and limited commitments as proposed for U.S. privacy law compliance.

Japan has an advantage when it comes to transfers to and from the EU. It received a mutual adequacy decision with the EU in 2019 — the first country to do so after the GDPR went into effect. This allows the transfer of personal data to the EU from Japan to be made freely, and from Japan to the EU with just a simplified contractual arrangement. New Zealand earned adequacy before the GDPR took effect, and South Korea expects to agree on mutual adequacy with the EU soon.

Finally, China's Personal Information Protection Law goes into effect Nov. 1 and has many aspects that are similar to the GDPR but does not fully synchronize with the GDPR or other jurisdictions' privacy

laws. It is believed that China will publish its own SCCs instead of accepting the new EU SCCs, but details are not yet available.

Conclusions and outlook

Data-processing agreements are both a sales and compliance topic for many organizations. Customers using cloud solutions hosted globally are being pressured by regulators, litigants, their data protection officers and various other stakeholders. Organizations across all jurisdictions and industries need to develop practical solutions for data-processing agreements that can be implemented through the data-processing chain. All feel an urgent need to simplify and standardize.

For all countries within and a few outside the EEA, the new SCCs offer opportunities for standardization. For countries that do not require or reward an expansion of the new SCCs, companies can deploy concise, consolidated data-processing terms that address descriptive national statutory requirements, ideally without repetition and unnecessary complexities.

Businesses need to work collaboratively on this topic and separate contracting for compliance, where their interests are largely aligned, from contracting for commercial risk allocation, where their interests tend to be diametrically opposed. Privacy professionals should take a holistic view and be sympathetic to each contracting party's position in the supply chain. It is in everyone's interest to document technical and organizational measures well, satisfy documentation requirements under data protection laws, clarify obligations, and avoid ambiguities, raising amorphous negligence claims in case of a security breach. Customer and service providers each need meaningful, written instructions regarding personal data processing to keep the customer in control, and both parties can rely on exceptions from transfer restrictions. Companies within and outside the EEA need the relevant information to document transfer impact assessments, and companies outside the EEA are better positioned to compile the relevant facts.

If organizations or individuals refuse to take compliance-focused, pragmatic and collaborative views, they risk becoming an unnecessary obstacle to data flows and economic cooperation. This will impact their ability to focus on many other — arguably, more important — data privacy protection tasks, such as data security, transparency, retention and deletion. They also risk paralyzing their compliance programs and hindering revenue generation. Not one size fits all, but basic principles highlighted in this article apply to most businesses.

Authors


Lothar Determann
IAPP Member Contributor


Helena Engfeldt, CIPP/E, CIPP/US
IAPP Member Contributor


Michaela Nebel, CIPP/E, CIPP/US
IAPP Member Contributor


Flavia Rebello
IAPP Member Contributor


Kensaku Takase
IAPP Member Contributor