Skadden

Privacy & Cybersecurity Update

European Commission Publishes Updated Draft of Standard Contractual Clauses

The European Commission (EC) has published updated draft versions of the Standard Contractual Clauses for the transfer of personal data outside of the EU.

In November 2020, the EC published a draft implementing updated versions of the Standard Contractual Clauses (New SCCs) for the transfer of personal data outside of the EU to third countries pursuant to Article 46(2)(c) of the General Data Protection Regulation (GDPR). In addition to the existing controller-to-processor (C2P) and controller-to-controller (C2C) clauses, the New SCCs include long-awaited processor-to-processor (P2P) and processor-to-controller (P2C) clauses. The New SCCs also directly address the "supplementary measures" required by the *Schrems II* decision,[1] and the recent recommendation[2] by the European Data Protection Board (EDPB) that provided guidance on such supplementary measures. Once the New SCCs are adopted by the EC, organizations will have a one-year grace period for implementation.

Background

Standard Contractual Clauses are one of the mechanisms under Article 46 of the GDPR by which personal data can be transferred outside of the European Economic Area (EEA). Adopted prior to the implementation of the GDPR, the current SCCs — in theory — provide appropriate safeguards for the transfer of data outside the EEA. While upheld as a valid transfer mechanism in *Schrems II*, the need for alignment with the GDPR makes the release of the New SCCs timely and welcome.

A Practical Approach to Data Transfers?

The New SCCs' inclusion of P2P and P2C clauses is notable, as previously there were no SCCs to govern such relationships despite the ubiquity of, in particular, processor-to-subprocessor transfers.

[1] Court of Justice of the European Union, *Data Protection Commissioner v Facebook Ireland Ltd & Maximillian Schrems* (Case C-311/18).

[2] Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, currently in draft form and open to public consultation.

Through the addition of P2P clauses, the New SCCs more accurately reflect the reality of contemporary data transfers where there are often multiple transfers of a particular piece of personal data (*e.g.*, controller to processor to sub-processor). The New SCCs adopt a modular approach, setting out clauses that have general applicability and allowing parties to "plug in" clauses that are applicable to their specific transfer scenario (*i.e.*, C2P, C2C, P2P, P2C).

While P2P clauses have been widely welcomed, the need for P2C clauses is less clear. Practically, it is difficult to envision many scenarios in which a processor would impose such clauses on a controller, making the inclusion of the P2C set of clauses therefore of less obvious benefit.

The practical approach to data transfers also is reflected in the ability for new parties to accede to an existing set of clauses by way of a "docking clause." This development should offer parties increased flexibility to streamline the contractual negotiation process and will save organizations from having to engage in contractual negotiations with multiple parties throughout the life cycle of the contract regarding the clauses.

Liability

The New SCCs make clear that in the event of a conflict between the New SCCs and the provisions of any other agreement between the contracting parties, the New SCCs will prevail. As parties will continue to supplement SCCs with separate data processing agreements, this hierarchy between the New SCCs and data processing agreements creates a potential issue with respect to liability. While liability caps in current data processing agreements tend to be the most contested feature of negotiations, the New SCCs flatly provide for uncapped liability in the event of a breach of the New SCCs. However, it is not clear whether this position on liability in the New SCCs would conflict with a cap on data protection liability agreed upon by parties to a related data processing agreement. This uncertainty must be clarified in the finalized set of New SCCs.

Notifications of Data Breach

Under the New C2C SCCs, a data importer is required to notify the competent supervisory authority and data exporter of a personal data breach if that breach is "likely to result in significant adverse effects." This "notification threshold" appears to be inconsistent with Article 33 of the GDPR, which requires controllers to notify the competent supervisory authority of a personal data breach unless it is "unlikely to result in a risk to the rights and freedoms of natural persons." It is not clear why the breach reporting threshold in the New C2C SCCs has not been aligned with that of the GDPR. To avoid uncertainty going forward, consistent language would be preferable.

The EDPB Recommendation

The *Schrems II* decision and the EDPB's recommendation have a clear impact on the New SCCs. For example, the data exporter is required to undertake and document transfer impact assessments (TIAs) to assess the level of protection afforded to personal data prior to any transfer to the data importer, and the data importer is required to notify the data exporter upon receipt of a data request from a public authority.

However, there are inconsistencies between the New SCCs and the EDPB's recommendation that will require clarification in the finalized New SCCs. For example, when assessing a data importer's ability to comply with its data protection obligations, the EDPB advocates an objective approach, instructing parties to "look into other relevant and objective factors, and not [to] rely on subjective ones such as the likelihood of public authorities' access[ing] [their] data in a manner not in line with EU standards." By contrast, the New SCCs are clear that parties must "take due account" of "any relevant experience with prior instances, or the absence of requests for disclosure from public authorities received by the data importer for the type of data transferred." It is hoped that in the final versions of the New SCCs and EDPB's recommendation that the EC and the EDPB, respectively, will align their positions on whether parties must take an objective or subjective approach when conducting diligence on the data importer.

Brexit

Since the New SCCs were not adopted before the end of the Brexit transition period (December 31, 2020), it is unclear how the New SCCs will feature in the U.K.'s post-Brexit data protection landscape. The U.K. Information Commissioner's Officer (ICO) has indicated at this stage that the New SCCs are currently under review. While the ICO is likely to follow the New SCCs once finalized, the post-Brexit era ICO could equally decide to implement them with some variations. This will be an area to monitor going forward.

Key Takeaways

- Through the addition of the P2P set of clauses and a "docking clause," the New SCCs reflect a more practical approach to data transfers that is attuned to modern business needs and complex data flows. However, this practical approach is not necessarily borne out in all aspects of the New SCCs, and it is hoped that key areas of uncertainty, particularly with respect to liability and "notification thresholds," will be clarified through the consultation process.
- The New SCCs have been influenced by, and should be read in conjunction with, *Schrems II* and the EDPB's recommendation. Given the close relationship between these key pieces of EU law, it is essential that the EC and the EDPB ensure their respective approaches to cross-border data transfers are aligned.
- Once the New SCCs are adopted, which reportedly will occur in early 2021, organizations can continue to rely upon the current SCCs for a one-year grace period (provided that any contract to which the current SCCs are attached remains unchanged during this period). What has triggered concern from organizations is the requirement to have to repaper all existing SCCs by the end of this period, which is a burdensome exercise both in time and cost. This has been echoed in the feedback provided by stakeholders thus far. As such, it remains to be seen whether a more lenient approach to this repapering obligation will be adopted in the finalized set of New SCCs.

Return to Table of Contents

European Council Establishes Cybersecurity Industrial, Technology and Research Competence Centre

The European Council has created a Competence Centre to combat cybercrime, uniting the EU's cybersecurity resources and experts in hopes of furthering the region's ability to combat cyberattacks and advance privacy safeguards.

The European Council, which is made up of a representative of each member of the EU, announced plans to create an EU-wide initiative to combat cybercrime called the Cybersecurity Industrial, Technology and Research Competence Centre, based in Bucharest, Romania, with the goal of uniting the various members' cybersecurity resources. Accordingly, there also will be a network of individual coordination centers in each nation. The Centre will bring together subject matter experts in areas such as industry, academia, research and the public sector, with its objectives including:

- contributing to the wide deployment of the latest cybersecurity technology, in particular through carrying out or supporting procurement of products and solutions;
- providing financial support and technical assistance to cybersecurity startups and small and medium-sized enterprises to connect them to potential markets and attract investment;
- supporting research and innovation based on a comprehensive industrial and research agenda, including large-scale research and demonstration projects in next-generation cybersecurity capabilities;
- driving high cybersecurity standards not only in technology and cybersecurity systems, but also in skills development; and
- facilitating the cooperation between the civil and defense sectors with regard to dual-use technologies and applications.

The EC has proposed the Competence Centre be funded jointly by financial contributions from the EU and the participating member states.

Key Takeaways

The Competence Centre is another example of how countries are seeking to pool their resources and expertise to combat cybercrimes. We will monitor the developments that come from the Centre and provide updates on any of its actions or recommendations.

Return to Table of Contents

California Attorney General Proposes Fourth Set of California Consumer Privacy Act Modifications

In December 2020, California Attorney General Xavier Becerra proposed a fourth set of modifications to the California Consumer Privacy Act (CCPA).[3] These new modifications build on the third set, which was released in October and are still not finalized.

Most of the changes proposed in the fourth set of modifications address the right of consumers to opt-out of the sale of their personal information, including the addition of a button

[3] See here to view the modifications.

that sites should use to signify an opt-out request. This button would be in addition to, and not in lieu of, posting notice of a right to opt-out or a "Do Not Sell My Personal Information" link. This button (shown below) would be placed to the left of the text where a business posts the "Do Not Sell My Personal Information" link, as required by the CCPA and subsequent attorney general regulations:

The proposed regulations also expand on the process by which businesses that collect personal data offline (*e.g.*, in a store) must provide notice of the right to opt out of a sale.

Key Takeaways

The attorney general's proposal is the latest in a set of modifications to the CCPA that have been brought to public attention. As the third set of modifications has yet to be finalized, it is possible that there will be even further modification suggestions as we go forward in 2021.

Return to Table of Contents

Privacy & Cybersecurity Update

Contacts

Stuart D. Levi
Partner / New York
212.735.2750
stuart.levi@skadden.com

James Carroll
Partner / Boston
617.573.4801
james.carroll@skadden.com

Brian Duwe
Partner / Chicago
312.407.0816
brian.duwe@skadden.com

David Eisman
Partner / Los Angeles
213.687.5010
david.eisman@skadden.com

Patrick Fitzgerald
Partner / Chicago
312.407.0508
patrick.fitzgerald@skadden.com

Todd E. Freed
Partner / New York
212.735.3714
todd.freed@skadden.com

Marc S. Gerber
Partner / Washington, D.C.
202.371.7233
marc.gerber@skadden.com

Rich Grossman
Partner / New York
212.735.2116
richard.grossman@skadden.com

Michael E. Leiter
Partner / Washington, D.C.
202.371.7540
michael.leiter@skadden.com

William Ridgway
Partner / Chicago
312.407.0449
william.ridgway@skadden.com

Jason D. Russell
Partner / Los Angeles
213.687.5328
jason.russell@skadden.com

David Schwartz
Partner / New York
212.735.2473
david.schwartz@skadden.com

Ingrid Vandenborre
Partner / Brussels
32.2.639.0336
ingrid.vandenborre@skadden.com

Helena Derbyshire
Of Counsel / London
44.20.7519.7086
helena.derbyshire@skadden.com

Jessica N. Cohen
Counsel / New York
212.735.2793
jessica.cohen@skadden.com

Peter Luneau
Counsel / New York
212.735.2917
peter.luneau@skadden.com

James S. Talbot
Counsel / New York
212.735.4133
james.talbot@skadden.com

Eve-Christie Vermynck
Counsel / London
44.20.7519.7097
eve-christie.vermynck@skadden.com

Skadden, Arps, Slate, Meagher & Flom LLP
One Manhattan West
New York, NY 10001
212.735.3000