AN A.S. PRATT PUBLICATION
JUNE 2021
VOL. 7 • NO. 5

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis

Pratt's Privacy & Cybersecurity Law Report

VOLUME 7 **NUMBER 5** **June 2021**

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please contact:
Deneil C. Targowski at 908-673-3380
Email: ..... Deneil.C.Targowski@lexisnexis.com
For assistance with replacement pages, shipments, billing or other customer service matters, please call:

Customer Services Department at ..... (800) 833-9844
Outside the United States and Canada, please call ..... (518) 487-3385
Fax Number ..... (800) 828-8341
Customer Service Web site ..... http://www.lexisnexis.com/custserv/
For information on other Matthew Bender publications, please call

Your account manager or ..... (800) 223-1940
Outside the United States and Canada, please call ..... (937) 247-0293

ISBN: 978-1-6328-3362-4 (print)
ISBN: 978-1-6328-3363-1 (eBook)

ISSN: 2380-4785 (Print)
ISSN: 2380-4823 (Online)

Cite this publication as:
[author name], [*article title*], [vol. no.] PRATT'S PRIVACY &CYBERSECURITY LAW REPORT [page number] (LexisNexis A.S. Pratt);
Laura Clark Fey and Jeff Johnson, *Shielding Personal Information in eDiscovery*, [7] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [143] (LexisNexis A.S. Pratt)

An A.S. Pratt Publication
Editorial

Editorial Offices
630 Central Ave., New Providence, NJ 07974 (908) 464-6800
201 Mission St., San Francisco, CA 94105-1831 (415) 908-3200
www.lexisnexis.com

MATTHEW BENDER

(2021–Pub. 4939)

Editor-in-Chief, Editor & Board of Editors

Pratt's Privacy & Cybersecurity Law Report is published nine times a year by Matthew Bender & Company, Inc. Periodicals Postage Paid at Washington, D.C., and at additional mailing offices. For customer support, please contact LexisNexis Matthew Bender, 1275 Broadway, Albany, NY 12204 or e-mail Customer.Support@lexisnexis.com. Direct any editorial inquires and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway Suite 18R, Floral Park, New York 11005, smeyerowitz@meyerowitzcommunications.com, 646.539.8300. Material for publication is welcomed—articles, decisions, or other items of interest to lawyers and law firms, in-house counsel, government lawyers, senior business executives, and anyone interested in privacy and cybersecurity related issues and legal developments. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

POSTMASTER: Send address changes to *Pratt's Privacy & Cybersecurity Law Report*, LexisNexis Matthew Bender, 630 Central Ave., New Providence, NJ 07974.

Cross-Border Personal Data Transfers: Proposed New SCCs Impose Significant Restrictions on Businesses

By Jenny Arlington, Jay Jamooji, Sahar Abas, Natasha G. Kohne, Michelle A. Reed, and Rachel Claire Kurzweil*

This article offers a high-level summary of two highly anticipated European Commission draft documents to facilitate data transfers.

The European Commission recently published two highly anticipated draft documents to facilitate data transfers.

The first was the new, updated, and modernized standard contractual clauses ("New SCCs")[1] for the transfer of personal data outside the European Economic Area ("EEA"), envisaged under Article 46 of the European Union General Data Protection Regulation (("EU") 2016/679) ("GDPR").

The second was the separate draft set of Article 28 standard contractual clauses[2] between controllers and processors, aimed at assisting companies located in the EU with the requirement for a contract between the controller and processor ("Article 28 Clauses").

If the New SCCs are as widely used as their predecessors (the standard contractual clauses implemented under the old Data Protection Directive, "Old SCCs"), any business involved in international personal data transfer would need to be familiar with these clauses. This article offers a high-level summary of the New SCCs.

FIVE HIGHLIGHTS FROM THE DRAFT NEW SCCs

It appears that two of the catalysts for the European Commission's decision to publish the draft New SCCs were (1) the landmark decision of the Court of Justice of the European Union *Schrems II* in July 2020, which significantly impacted international personal data transfers, and (2) the developments taking place in the digital economy,

* Jenny Arlington (jarlington@akingump.com) is counsel at Akin Gump Strauss Hauer & Feld LLP. Jay Jamooji (jay.jamooji@akingump.com), Sahar Abas (sahar.abas@akingump.com) and Rachel Claire Kurzweil (rkurzweil@akingump.com) are associates at the firm. Natasha G. Kohne (nkohne@akingump.com) and Michelle A. Reed (mreed@akingump.com) are partners at the firm and are co-heads of its cybersecurity, privacy, and data protection practice.

[1] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12741-Commission-Implementing-Decision-on-standard-contractual-clauses-for-the-transfer-of-personal-data-to-third-countries.

[2] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12740-Commission-Implementing-Decision-on-standard-contractual-clauses-between-controllers-and-processors-located-in-the-EU.

including new and more complex processing activities, which necessitated an update to the Old SCCs (which had last been updated in 2004, for controller-to-controller, and in 2010, for controller-to-processor transfers).

The terminology in the Old SCCs is kept in the new proposal: "data exporter" is the entity which is transferring personal data out of the EEA; "data importer" is the entity which is receiving that data in a non-EEA country.

Businesses would need to consider the New SCCs in detail once they become final, but at this stage there are five highlights that may be of particular interest.

1) *In comparison with the Old SCCs*: The Old SCCs are clauses that would usually take eight or nine pages, and would be incorporated as an annex to a "head agreement" governing the parties' business relationship. The New SCCs span 29 pages (even if this encompasses various "modules," see below); there is still an express provision that they may be incorporated into broader contracts, but it remains to be seen how this could be done most efficiently bearing in mind the length of the clauses. At a substantive level, the proposed clauses in the New SCCs are more detailed, more involved, impose more obligations and regulate more aspects of the data exporter-data importer relationship than the Old SCCs.

2) *Parties*: The limited choice of parties and business relationships available under the Old SCCs has been expanded. The draft New SCCs offer four various options, so-called "modules," to capture the possible relationships between the parties: controller-to-controller, controller-to-processor, processor-to-processor, and processor-to-controller transfers. The New SCCs envisage further expansion of the parties to the clauses, as they include a "docking clause." That would allow controllers and processors (such as in the case of onward transfers of data) to accede to the clauses, as additional data importers or exporters, throughout the life cycle of the relevant contract.

3) *Schrems II*: Two clauses in Section II of the draft New SCCs[3] seem to be devoted to specific compliance with *Schrems II*. They set out various obligations that the parties agree to and warrant in respect of local laws affecting compliance with the clauses, and specific obligations on the data importer in case of government access requests. In particular, the New SCCs propose an obligation on data exporters and importers to conduct a thorough assessment to determine whether the data importer in the third country can truly guarantee an adequate level of protection for transferred personal data. The European Data Protection Board Taskforce's recommendations, when finalized, would be intertwined with these provisions. Further, some of the proposed obligations on the data importer (i.e., the party in a non-EEA

[3] Clause 2 and 3.

country receiving the personal data) are particularly onerous. For example, the data importer agrees to review the legality of a request by the non-EEA government for disclosure of EEA individuals' personal data and "to exhaust all available remedies to challenge the request."[4]

4) *Cybersecurity*: The Old SCCs required that technical and organizational security measures must be taken by the data controller that are appropriate to the risks, such as against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, presented by the processing. The draft New SCCs reiterate the need for security of processing, by adding no fewer than 17 categories of technical and organizational measures that the data importer needs to describe in Annex II.

   These categories include, for example, description of the data importer's requirements for internal IT and IT security governance and management; its requirements for data avoidance and minimization; and its requirements for data quality. In addition, it is proposed that the data importer would need to notify both the data exporter and the competent supervisory authority in case of a data breach, something which goes over and above the notification requirements under the GDPR. The proposed threshold for notification also appears different from the GDPR requirements: the New SCCs refer to notifications in case the breach "is likely to result in significant adverse effects," whereas the GDPR notification provisions refer to the likelihood of risks to individuals' rights and freedoms.

5) *Sub-processors:* A few of the proposed clauses in the New SCCs envisage, in the case of a processor-to-processor transfers, greater involvement and supervision by the ultimate data controller. For example, one of the proposed requirements is that the sub-processor data importer should provide, at the processor data exporter's request, *or* at the data controller's request, a copy of the sub-processor agreement and subsequent amendments.[5] The GDPR does not provide for such an invasive disclosure; the GDPR merely states that where the sub-processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that sub-processor's obligations.[6]

[4] Clause 3.2(a), Section II.
[5] Clause 4(c), Module 3, Section II.
[6] Article 28(4).

SUBSTANCE OF THE PROPOSED ARTICLE 28 CLAUSES

The second set of draft clauses published by the European Commission relate to Article 28 of the GDPR, which regulates a data processor's activities, while processing data on behalf of a data controller. Among other things, Article 28 requires that there should be a contract between the processor and the controller that satisfies the requirements of Article 28(3) and 28(4) of the GDPR.

Article 28(7) of the GDPR had envisaged that the European Commission may publish "standard contractual clauses" which would set out what that Article 28 contract was supposed to include. At the time the GDPR was adopted, there was no such publication. Now, with over two years of the GDPR in force, the European Commission has published the proposed clauses for such a contract. Entering into the proposed Article 28 Clauses is not compulsory: parties are allowed to enter into another agreement, as long as that satisfies the GDPR requirements set out in Article 28 thereof.

In certain places, the draft Article 28 Clauses follow the proposals in the New SCCs, such as the requirement on the processor to describe at least 17 categories of technical and organizational measures that it has adopted to safeguard the security of the data processing. Article 28 Clauses however would not be implemented where there is an international personal data transfer; they only regulate personal data processing within the EEA. The European Commission has clarified that where personal data is being transferred outside the EEA, entering into the New SCCs would also satisfy the requirement to have a controller-processor contract under Article 28(3) and (4) of the GDPR.

COMMENTS BY THE EDPB AND EDPS AND NEXT STEPS

The European Commission sought and received feedback on its drafts through a public consultation which closed on December 10, 2020. On January 15, 2021, the European Data Protection Board ("EDPB") and the European Data Protection Supervisor (the independent data protection authority monitoring EU institutions) ("EDPS") announced that they had provided their joint opinions on the two draft sets of contractual clauses to the European Commission. The two bodies highlighted that their comments on the proposals included requests for more clarity to the text of the drafts, to ensure their practical usefulness in day-to-day operations.

In particular, the European Commission was invited to provide further clarity on the scope of the draft New SCCs, the proposed obligations regarding onward transfers, certain aspects of the envisaged assessment of third country laws, the so-called "docking clause," the roles and responsibilities of each of the parties to the proposed contracts, certain third party beneficiary rights and the proposed clauses dealing with notifications to the data protection regulators. It appears that finalizing the drafts may take some time.

Under the current proposal, once the New SCCs concerning international data transfers are finalized and adopted, the New SCCs will become effective immediately. However, for a period of one year from the date the New SCCs are adopted, data exporters and data importers may continue to rely on the Old SCCs for the performance of a contract entered into before the adoption of the New SCCs, provided certain conditions are met.

Given the wide use of the Old SCCs (the recently published International Association of Privacy Professionals – FTI Consulting Privacy Governance Report 2020 indicates that 88 percent of firms that transfer data outside the EU do so on the basis of the Old SCCs), the impact of any amendments to the framework is likely to be significant.

Notably, the proposed detailed data security and other obligations on data importers may require fundamental technical and organizational changes, especially in light of the updated clauses aimed at guaranteeing an effective enforcement of third-party rights.