Lowenstein Sandler

Privacy & Cybersecurity

January 29, 2021

Post-Brexit, *Schrems II*, and the GDPR: Privacy Compliance Priorities in Early 2021 (Part Two)

By Mary J. Hildebrand CIPP/US/E, Edgar R. Hidalgo CIPP/US, and Carly S. Penner CIPP/US

As we began exploring last week in ***Part I of our Post-Brexit, Schrems II, and the GDPR: Privacy Compliance Priorities in Early 2021*** series, significant developments in late 2020 charted a course in privacy/cyber compliance for companies doing business in the European Economic Area (EEA) to take in early 2021. New guidance was issued by the European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS), and the European Commission released new versions of Standard Contractual Clauses (SCCs) for public comment. In Part II of our series, we will examine the implications of these developments in the wake of the Schrems II decision and their impact on data transfers from the EEA to the United States ("U.S.").

Part II: *Post-Schrems II* Regulatory Guidance and Draft SCCs

Supplementary Measures

While the Court of Justice of the European Union (CJEU) made clear in the *Schrems II* decision that simply relying on existing SCCs as a valid transfer mechanism in the wake of the invalidation of the EU-US Privacy Shield would not be enough to comply with data transfer rules, the CJEU failed to define what else would be needed to comply. In its decision, the CJEU suggested that companies relying on SCCs would need to implement "supplemental measures" to ensure that personal data would be adequately protected when transferred from the EEA to a country deemed to provide insufficient protection, but the court did not expound on what those supplemental measures would involve.

In response to the *Schrems II* decision, on November 10, 2020, the EDPB released recommendations regarding supplemental measures, describing them in three categories: contractual, technical and organizational. Like the *Schrems II* court, the EDPB made clear that contractual measures alone would not be enough to meet the *Schrems II* standard and emphasized the importance of technical measures such as encryption and pseudonymization, as well as the prevention of government access to personal data. Importantly, the EDPB also made clear that the sufficiency of supplemental measures would be determined, not on the amount or complexity of the measures, but rather on their effectiveness when weighed against the risks attendant to each particular data transfer. The EDPB's guidance, in effect, requires companies to: (1) assess the risks involved in each data transfer, (2) implement supplemental measures in response to such risks to protect data subjects, and (3) audit, monitor and evaluate, on a case-by-case basis, whether the implemented measures actually provide more protection against the risks presented by data transfers.

Proposed Form SCCs

On November 11, 2020, for the first time in nearly 20 years, the European Commission published new versions of the SCCs: one set of SCCs address the transfer of personal data from an EEA country to a non-EEA country (New Data Transfer SCCs), and the second set of SCCs is intended to standardize GDPR Article 28 obligations for controllers and processors (EC Model DPAs).

Although the Article 28 requirement of entering into data processing terms has been a central component of GDPR compliance for controllers and processors alike since the regulation became effective in 2018, the European Commission has not proposed standard terms until now despite having the authority to do so. In the absence of any action by the European Commission, certain member country data protection authorities, such as in the Netherlands

and Denmark, have published data processing templates on their own and it has become common practice for regulated companies to establish their own form data processing agreements. One of the goals of the EC Model DPAs is to "ensure full harmonisation and legal certainty across the EU when it comes to contracts between controllers and their processors." These EC Model DPAs include annexes for descriptions of the processing, the technical and organizational measures to secure the personal data, data controller instructions for processing the personal data, specific processing restrictions for special categories of data, and a list of subprocessors. Importantly, however, the EC Model DPAs will be made available to controllers and processors to use at their discretion, and the terms can be enhanced, changed or modified to fit particular scenarios as the regulated businesses may agree. The EC Model DPAs signals the level of specificity and detail expected by the European Commission when controllers and processors enter into Article 28 data processing agreements and may function as a guide to regulated entities.

Unlike the EC Model DPA, the New Data Transfer SCCs are intended to replace and improve on the current form data transfer SCCs. Whereas the current form data transfer SCCs only addressed two types of data transfers— data transfers from an EEA controller to a non-EEA controller and an EEA controller to a non-EEA processor— the New Data Transfer SCCs contemplate other scenarios— transfers from an EEA processor to non-EEA controller and an EEA processor to a non-EEA processor. The addition of these data transfer combinations seeks to resolve some of the issues non-EEA located businesses encountered when trying to rely on the current form SCCs (i.e., neither current form SCC really works for a data transfer between a non-EEA established data controller and a data processor located in the EEA or transfers between two processors).

Most recently, on January 15, 2021, the EDPB and the EDPS adopted joint opinions on these two sets of new form SCCs concluding that the drafts presented a "reinforced level of protection for data subjects" while also noting that some provisions could be improved or clarified. The joint opinion highlighted that the New Data Transfer SCCs better reflected the current reality that data processing has become more complex and involves different types of data importers and exporters. According to the draft of the EU Commission Implementing Decision for the New Data Transfer SCCs, entities that rely on SCCs for data transfer have one year from the date the New Data Transfer SCCs are finalized and adopted to replace the older form SCCs. Note, however, the EDPB requested several amendments to the new SCCs to bring more clarity to the roles and responsibilities of controllers and processors, and the period for public comment on the new SCCs recently ended, so these current drafts are not yet final.

As we await the finalization and approval of the New Data Transfer SCCs, it is important to remember that these new SCCs do not represent a total fix for data transfers, and that the need to implement supplementary measures described by the CJEU in *Schrems II* remains. EDPB Chair Andrea Jelinek noted in the EDPB/EDPS joint opinion that many companies will still need to implement supplementary measures "to ensure that data subjects are afforded a level of protection essentially equivalent to that guaranteed within the EU" and that the EDPB recommendations on supplementary measures discussed above should be used in conjunction with the New Data Transfer SCCs once finalized.

Collectively, these recent developments recommend that U.S. businesses that transfer personal data from the EEA to the U.S. should promptly:

- conduct a risk assessment of such data transfers;
- analyze and implement appropriate contractual, organization and technical measures based on such assessment to supplement reliance on SCCs as the valid data transfer mechanism in accordance with EDPB guidance; and
- remain alert for the adoption of final New Data Transfer SCCs which will need to be executed within the year.

About Us
In today's digital world, where data has become a key asset for conducting business, companies continue to face greater privacy and cybersecurity challenges. At Lowenstein Sandler, our Privacy & Cybersecurity team helps clients navigate the rapidly evolving, increasingly complex privacy and security law landscape in the United States, the EU, and around the world. We deliver innovative privacy and security solutions that meet our clients' critical business needs including the commercialization of data assets in a legally compliant manner. Our targeted counsel is relevant to companies across diverse industry sectors, and public and private companies from start-ups to global enterprises.

Contacts

Please contact the listed attorneys for further information on the matters discussed herein.

MARY J. HILDEBRAND CIPP/US/E
Partner
Chair, Privacy & Cybersecurity
T: 973.597.6308
mhildebrand@lowenstein.com

EDGAR R. HIDALGO CIPP/US
Counsel
T: 973.422.6418
ehidalgo@lowenstein.com

CARLY S. PENNER CIPP/US
Associate
T: 973.597.2516
cpenner@lowenstein.com