GODFREY & KAHN S.C.

December 2020

Guidance from the EDPB on Schrems II *and future changes to trans-border data flows and standard contractual clauses*

Kate Campbell
414.287.9529
kcampbell@gklaw.com

Sarah A. Sargent
414.287.9450
ssargent@gklaw.com

Justin P. Webb
414.287.9527
jwebb@gklaw.com

The pace at which global privacy laws and guidance are evolving has not slowed during the 2019 novel coronavirus (COVID-19) pandemic, especially with respect to the General Data Protection Regulation (GDPR). European data regulators have issued additional guidance for businesses that transfer personal data out of the European Economic Area in light of this summer's Schrems II ruling.

On July 16, 2020, the European Court of Justice issued a ruling (Schrems II) that invalidated the EU-US Privacy Shield on which many companies relied to transfer their data between the US and EU. The Schrems II ruling did not invalidate the use of Standard Contractual Clauses (SCCs) as a global data transfer mechanism but did create some uncertainty around their use. The ruling held that SCCs may only be relied upon if the safety of EU citizens' data can be guaranteed. What that meant and how that could be accomplished was subject to much discussion and debate until last month, when the European Data Protection Board (EDPB) released 38 pages of guidance. The EDPB's guidance has not stopped the global discussion about whether the restriction of trans-border data flows is unreasonable, but it has provided some guidance on how to comply with Schrems II.

Specifically, the EDPB's guidance provides companies a set of six steps to follow in order to assess whether a company's international data flows are compliant with EU law (including Schrems II) and provide an "EU level of protection of personal data." These six steps are:

1. Mapping of international data transfers
2. Verifying your transfer tools
3. Assessing whether the laws of the destination country "may impinge on the effectiveness of the appropriate safeguards of the transfer tools you are relying on, in the context of your specific transfer"
4. Identifying and adopting supplementary measures to provide the essential equivalent of protection under EU law
5. Taking any formal procedural steps to adopt the supplementary measures
6. Re-evaluating periodically the level of data protection and monitoring any relevant developments

With these recommendations in mind, companies using SCCs for their international data transfers should be assessing their data flows and use of SCCs, and developing supplementary measures to address US surveillance efforts that may be inconsistent with EU notions of privacy, as addressed in Schrems II.

Looking to the future of SCCs, regulation changes are likely to come early next year. The European Commission has issued a draft decision regulating the use of SCCs for the international transfer of personal data and opened a Feedback Period that ends Dec. 10, 2020. The final iteration of this decision is expected in the first quarter of 2021. The newly proposed SCCs cover controller-to-controller, controller-to-processor and processor-to-processor data flows. The proposed SCCs are also much more robust than the previous version issued by the European Commission many years ago. Companies using SCCs will most likely need to update all their contracts that include SCCs or at the very least use the new SCCs once they are released.

Godfrey & Kahn's Data Privacy and Cybersecurity Group continues to monitor the European Commission's decisions and guidance on SCCs, as well as the latest developments impacting GDPR.

If you need assistance with developing a plan to comply with Schrems II and the EDPB guidance, understanding the new SCCs or updating your SCCs to the new form, please reach out to a member of our team.