GROOM LAW GROUP

Publications

European Privacy Regulators Propose Rules for Data Transfers to the U.S.

ATTORNEYS & PROFESSIONALS

Kevin L. Walsh
kwalsh@groom.com
202-861-6645

PUBLISHED
11/20/2020

SOURCE
Groom Publication

SERVICES

- Retirement Programs
- Fiduciary & Plan Governance
- Health & Welfare Programs
- Plan Services & Providers

On November 10, 2020, the European Data Protection Board ("EDPB") released proposed rules describing the conditions that entities subject to the European Union's ("EU") General Data Protection Regulation ("GDPR") can transfer data to third countries (the "Proposal"). The Proposal is significant because it follows a recent judgement of the Court of Justice of the European Union ("CJEU") that held that prior rules governing EU data transfers to the United States were inadequate. If you are a multinational employer with a European presence or a service provider to European retirement or health plans, it will be important to track these rules as they evolve and to begin to develop new compliance mechanisms.

On July 16, 2020, the CJEU invalidated the EU-U.S. Privacy Shield on the grounds that it had inadequate protections, in part based on access by U.S. intelligence services to data. Following that decision, the EDPB released the Proposal reminding EU entities that "transferring personal data to third countries cannot be a means to undermine or water down the protection it is afforded in the EEA." As an example, the EDPB called out transfers to the U.S. stating that "Section 702 of the U.S. FISA [the Foreign Intelligence Surveillance Act] does not respect the minimum safeguards … [and] is not essentially equivalent to the safeguards required under EU law." As a result, the Proposal would make transfers to the U.S. subject to a six-step process that would necessarily involve "technical measures [to] make access to the data transferred impossible or ineffective."

I. The Six-Step Process for Data Transfers

Under the Proposal, exporters of data would be required to satisfy a six-step process before transferring data to the U.S., or another third country.

First, an exporter would be required to know their transfers. This not only includes knowing what personal data is transferred and who whom, but also what is then transferred on to additional third parties. In mapping the data that is transferred, the exporter would be required to verify that the data is adequate, relevant, and limited to what is necessary for the purpose it is being transferred and processed for.

Second, an exporter would be required to either (1) conclude that the European Commission ("EC") has issued an "adequacy decision" regarding the country to which the data is being transferred or (2) rely on a transfer tool. If the EC has, the exporter would not need to go through steps three through five. As described above, the U.S. has not received an adequacy decision (and has in fact been described as inadequate multiple times by the CJEU).

Under GDPR, there are five commonly used transfer tools:

- Standard data protection contractual clauses (which continue to evolve; the most recent draft issued by the EC on November 12, 2020, for comment can be found here)
- Binding corporate rules
- Codes of conduct
- Certification mechanisms
- Ad hoc contractual clauses

Third, the exporter would be required to assess whether there is anything in the law or practice of the data recipient country that would impinge on the effectiveness of the transfer tool. In performing this analysis, exporters are not allowed to rely on subjective factors such as the likelihood that the local government would have any interest in accessing the data. The EDPB cautions exporters to pay particular attention to laws that require access or disclosure to public authorities for law enforcement, regulatory purposes, or national security purposes. Where those laws exist, the EDPB states that any requirements must be "limited to what is necessary and proportionate in a democratic society." Further, where countries do not have national privacy laws, exporters should look to other relevant and objective factors.

Fourth, the exporter would be required to identify and adopt supplemental measures that are designed to bring the level of protection into equivalence with EU standards. Here, the EDPB expressly cautions that in some cases this may be impossible and that the exporter must then, "avoid, suspend or terminate the transfer to avoid compromising the level of protection of the personal data." The EDPB provides an extended list of possible supplemental factors but does not identify whether any or some combination would be sufficient to counteract the problematic nature of FISA Section 702.

Fifth, the exporter would be required to take any formal procedural steps required by the transfer tool being used.

Sixth, the exporter would be required monitor and periodically reevaluate whether the level of protection afforded to the data remains appropriate.

II. Conclusion

We will continue to monitor developments under GDPR to assist plan sponsors and service providers address cross-border pension issues.

European-Privacy-Regulators-Propose-Rules-for-Data-Transfers-to-the-U.S.