msk

european union - united states reach privacy deal

MSK Client Alert

February 9, 2016

As was widely reported last week, United States and European Union officials announced that terms of a "Safe Harbor 2.0" has been reached. Now called the "EU-US Privacy Shield," few tangible details are public at this time. Thus, the approximately 4,400 companies that are currently Safe Harbor compliant remain in limbo, waiting for the full terms of the Privacy Shield to be drafted and (hopefully) approved. In the interim, affected companies are trying to determine the best ways to lawfully transfer personal data between the E.U. and the U.S. in anticipation of new rule implementation.

To date, the only "official" information can be found in a press release from Commerce Secretary Pritzker, see Commerce Privacy Shield Release, a similar short press release from Federal Trade Commission Chair Edith Ramirez, see FTC Privacy Shield Release, and one from European Commissioner for Justice Věra Jourová, see EU Privacy Shield Release. Per these sources, the Privacy Shield provides for an annual joint review, plus mechanisms for independent oversight, individual redress and a U.S. mechanism for EU citizens to resolve their complaints against American companies. The EU release also contains some noteworthy language about the U.S. committing in writing that no "indiscriminate mass surveillance" will occur, that access by U.S. authorities (read CIA, NSA, etc.) to personal data from Europe will be limited to "what is necessary and proportionate," and that safeguards for individuals will apply equally to EU citizens. Of course, as the EU correctly points out, this is not a treaty but an exchange of letters, so enforcement will be made more complicated by that fact.

In advance of specific terms being adopted, details about the contents of the agreement can be interpreted from interviews and unofficial comments. For example, on February 4, 2016, the Information Technology and Innovation Foundation interviewed FTC Commissioner Julie Brill. During the interview, Comm. Brill explained that EU citizens with complaints about how their data is processed in the U.S. can now go directly to the American company involved, engage in alternative dispute resolution (including arbitration), go to their

attorneys

Susan Kohn Ross

practice areas

cybersecurity and privacy

regulatory

country's Data Protection Authority (DPA), or file a complaint with the FTC. Also noteworthy, Comm. Brill indicated the Privacy Shield process will contain protections for onward data transfers that apply to both the party transferring the EU data, as well as the U.S. party receiving it. Thus, companies will need to carefully review their existing protocols against the new requirements, once they are published.

In the interim, uncertainty remains as to what companies, which are transferring data to the U.S., need to do to avoid enforcement actions. Standard contractual clauses and binding corporate rules remain valid transfer mechanisms that companies may rely on, but compliance with the old Safe Harbor may not necessarily be acceptable. Indeed, while Comm. Brill has stated the FTC will continue to enforce the old Safe Harbor's pre-existing conditions and expects companies to abide by those principles while the Privacy Shield is being implemented, the EU's Article 29 Working Party has stated that transfers made under the old Safe Harbor are no longer valid. The Working Party, however, has left it to individual member state DPAs to decide how to deal with complaints regarding any ongoing transfers. In this regard, it is unknown how all of the DPAs will proceed. For example, certain DPAs (e.g., Switzerland and Estonia) have stated they will not bring enforcement actions against companies which are compliant with the old Safe Harbor while the terms of the Privacy Shield are finalized, whereas others (e.g., France and Holland) have been vague as to their intentions.

As to when the full terms of the Privacy Shield will be written and made public, the Article 29 Working Party has asked to receive the text by the end of February, in advance of its March meeting. The goal would be for the Working Party to review and approve the terms (if it does indeed approve them) by mid-to-late April. This, however, is definitely a "do not hold your breath" moment. There is no guarantee this timetable will be met, or that the Working Party will agree to the terms as drafted. As is typical of government negotiated deals, the practical consequences are seldom as originally envisioned by the negotiators. Thus, for now, companies must decide whether to implement the more expensive and burdensome standard contractual clauses and binding corporate rules or, at the very least, to continue meeting the requirements of the old Safe Harbor while hoping for the best until the Privacy Shield is finalized. In either respect, companies should make sure they are comfortable with their existing compliance protocols, be ready to act quickly to conform their protocols if and when the Privacy Shield is approved, and ask themselves the following questions:

1. Are you transferring private data about individuals from the EU to the US?
2. If so, are you employing standard contractual clauses and binding corporate rules and, if not, do they make sense for your operation as a means to reduce potential risk?
3. Absent such measures, are your current privacy protection protocols at least compliant with the old Safe Harbor requirements?
4. Are you currently registered under the Safe Harbor? If not, and you are eligible, have you properly documented the reasons for the decision not to register with the Department of Commerce?
5. If you are relying on adherence to the old Safe Harbor requirements, for each individual EU member state from which you are transferring private data, do you know the position of that member state's DPA on whether it will bring enforcement actions while the Privacy Shield is being analyzed and (potentially) adopted?

Are your protocols being followed? If not, what changes need to be documented or implemented?

los angeles
t 310.312.2000
f 310.312.3100

new york
t 212.509.3900
f 212.509.7239

washington, dc
t 202.355.7900
f 202.355.7899