Author:

Dr. Ulrich Baumgartner
LL.M. (King's College London), CIPP/E | Partner

02.04.2025

The end of the DPF might be around the corner – What companies should do now

In summary:

In this blog post on the current turbulences around the EU-U.S. Data Privacy Framework ("DPF"), we spoke with our dear colleague Travis LeBlanc, one of the former members of the U.S. Privacy and Civil Liberty Oversight Board ("PCLOB") who has been dismissed by the new U.S. Administration. Travis was skeptical regarding the future of the DPF but also said that in his view it is too early to predict it with a reasonable degree of certainty. In this second part of our newsletter, we look ahead and share some advice on what EU companies and organizations can and should do to prepare for the potential discontinuation of the DPF.

1. The Current State of Play on the EU Side

But let's take a look on the state of play on the European side first.

By way of a recap, there are two players who could bring down the DPF: the European Court of Justice ("CJEU") and the EU Commission, on whose "adequacy decision" the DPF relies. There are several challenges against the DPF currently making their way to the CJEU. However, it will likely take a while until the CJEU rules on the DPF. Therefore, all eyes are currently on the EU Commission and their reaction to the developments in Washington D.C. At the time of writing this newsletter, the EU Commission seems determined to continue with the DPF. This was made clear just a few days ago by the competent EU. Commissioner Michael McGrath. "It is an objective of the EU to continue with full implementation and enforcement of the DPF" he stated publicly during a webinar. Nevertheless, the pressure on the European Commission is increasing, not least from the side of the EU Parliament. In our view, the current situation on the U.S. side seems to be just about acceptable to the EU Commission. However, any further weakening of the legal redress mechanism in the U.S. or even changes to the Executive Order 14086 or other statutes underlying the DPF will likely force the EU Commission to rethink the DPF.

Also, the EU's national data protection supervisory authorities have published several pieces of guidance over the last weeks, confirming that they continue to accept data transfers on the basis of the DPF (just two days ago, the Dutch regulator came out with such a statement). However, this should not obscure the fact that the supervisory authorities are – by their nature – increasingly critical of the DPF. Bear in mind that the supervisory authorities have a 'sharp sword' in their hands that has often been overlooked so far. According to Section 21 of the German Data Protection Act (which is based on Art. 58(5) GDPR, so similar provisions exist in other EU member state laws), the German supervisory authorities must have adequacy decisions of the EU Commission that they consider to be unlawful reviewed by the courts. The German Federal Administrative Court is responsible for review, which in turn would have to refer any doubts about the legality of an adequacy decision to the CJEU by way of a request for a preliminary ruling. In our view, it is only a matter of time until a (German) regulator takes such a step.

2. A Call to Action for EU Companies

Taken together, therefore, it seems only prudent for EU organizations to prepare for the potential end of the DPF. Here are a few thoughts on what to do now:

First and foremost, every data transfer to the U.S. that can be avoided will make life easier going forward (even if the DPF should survive in the short term). While it is, of course, unrealistic for most companies to switch to EU-based service providers (if there are any real alternatives at all), our experience shows that some transfers often can be switched off rather easily. Intra-group data transfers in particular can often be reduced by simply readjusting access rights or roles and responsibilities of employees of non-EU group companies. Therefore, a fresh look at existing data transfers to the U.S. is always the first step.

Secondly, EU companies should take a careful look at the server locations of their indispensable U.S. providers. And do not forget access rights to EU servers by support staff or other personnel located in the U.S. – something which might qualify as a "data transfer." Some major U.S. cloud and other technology providers have strengthened their localization efforts and offer "local services" out of the EU. But be careful: Not every "EU Boundary" or other localization solution eliminates at least occasional data transfers to a U.S. parent company. It is incredibly burdensome for U.S.-based providers to offer their services exclusively out of the EU with the same quality (and price tag). Therefore, certain localization claims turn out to be more marketing language than reality. It takes experience to ask the right questions.

Thirdly, if you have identified all "must-have" data transfers to the U.S., take a second look at whether they really qualify as "data transfers" as understood by the GDPR. The GDPR does not define this key term – and EU data protection supervisory authorities tend to interpret the concept of a data transfer way too broadly (although there is also some helpful EDPB guidance on this subject). That said, it might be possible to argue there is no "data transfer" if there is no real "recipient" of the data on the U.S. side – e.g., because data is only routed through the U.S. for technical reasons – or there are no technical means to access the data in the U.S. – e.g., if the data cannot be exported there.

Fourthly, for any "real" data transfers to the U.S. that remain after these initial three steps, companies should double-check they have a fallback option to the DPF available. The obvious choice are the EU Commission's Standard Contractual Clauses, which companies should have in place in addition to a DPF certification of their U.S. providers. But other safeguards will also do the job, like BCR or the derogations in Art. 49 GDPR which are often overlooked. If there are data transfers without such fallback option, companies should become active now and put in place alternative safeguards.

Finally, companies should prepare themselves to go back to the "dark days" after the CJEU's Schrems II ruling and start asking their U.S. providers for details of their "supplementary measures". Also, the acronym "TIA" might be something we all have to get used to again.