Author:

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

18.03.2025

International data transfers revisited – Open questions despite the DPF

In summary:

Even after the DPF takes effect, some question marks remain when transferring personal data to recipients outside the EEA. Two very recent publications of German supervisory authorities have raised eyebrows. We summarize some practical issues below and offer practicable solutions.

1. What is a “transfer” of data?

Although the EDPB has tried to clarify the concept of a “data transfer” in their updated Guidelines 05/2021, some questions remain which are highly relevant in practice.

First, it is still unclear whether a merely theoretical ability to access data stored within the EEA from a location outside of the EEA (e.g. by a remote support service technician in a third country) qualifies as a “transfer” of data to the technician. This seems odd, given that in many scenarios access to the data will be neither necessary nor intended by the parties. Nevertheless, the EDPB held that a scenario of mere theoretical access constitutes a “transfer”. But good news has come from the supervisory authority of the German state of Baden-Wuerttemberg in a guidance document published just last week. The regulator says that a mere factual ability to access can qualify as a “transfer” at least when there is factual access. In other words: (i) not every case of theoretical access leads to a transfer, and (ii) there may be no transfer whatsoever if the data is not actually accessed. Although this guideline (to our knowledge) has not been coordinated with other German supervisory authorities (let alone the EDPB), it confirms our experience in practice that it can be argued more often than expected that no “transfer” of data takes place in certain scenarios. Another example is the lack of a “processing activity” on the part of the data recipient in a third country, e.g. where data is only routed through a server operated by a company in a third country without the latter actually touching or processing the data (a common scenario in IP package routing, for example). Moreover, it may be possible to avoid a “transfer” by structuring a disclosure of personal data as a direct collection of personal data from the data subject by an entity outside the EEA – with the effect that there is no “data exporter” (the data subjects themselves do not qualify as data exporters). This shows that it is worth taking a closer look at whether there is really a data transfer at hand to avoid unnecessary time and effort.

2. DPF and SCC in parallel?

U.S. tech providers who relied on the EU standard data protection clauses (SCCs) pursuant to Art. 46(2)(c) GDPR before the DPF arrived typically continue to agree SCCs with their EU customers (or have not terminated SCCs dating back to pre-DPF times). At the same time, most major U.S. tech providers have swiftly certified under the DPF and thus use the DPF as a transfer mechanism according to Art. 45 GDPR. The reasons for such a "belt and braces approach" are obvious: No one can rule out a "Schrems III" decision of the CJEU and companies – understand-ably – want to be prepared for such a scenario by being able to fall back on SCCs, should the DPF be invalidated. Is this a problem? The Bavarian data protection supervisory authority (in their annual report for 2023, published a few days ago) says 'yes' – unless it is clearly stated that the DPF prevails and that the SCCs will only become effective as a transfer mechanism should the DPF be invalidated again. We don't fully follow the legal reasoning of the Bavarian regulator in arriving at this conclusion which seems to be an overly strict interpretation of Art. 46(1) GDPR (and neither does the prevailing opinion in legal literature). Nevertheless, at least for newly concluded contracts it seems advisable to include a clause on the "precedence" of the DPF over the SCCs – while retaining the additional protection afforded by keeping SCCs as a fallback. Legacy SCC contracts, however, require careful consideration.

3. Do not forget a data processing agreement!

The DPF does not ensure compliance with Art. 28 GDPR in a controller-to-processor scenario, unlike the SCCs (Module 2) which had the Art. 28 GDPR requirements incorporated. So, does this mean that a switch from SCCs to DPF requires the conclusion of a standalone data pro-cessing agreement? The answer is no, provided that the SCCs (Module 2) are in place alongside the DPF certification. In this case, regulators and the EU Commission take the view that the SCCs continue to satisfy the requirements of Art. 28 GDPR, even if the SCCs are replaced by a valid DPF certification as a mechanism for international data transfers (which creates some challenges for contract drafting). This is another good reason to leave existing SCCs in place. However, if SCCs (Module 2) are not in place, you will need a separate data processing agreement.

4. TIA or no TIA?

Finally, bear in mind that where there is a data transfer to a U.S.-based recipient not certified under the DPF, EU supervisory authorities still expect a TIA – as the Bavarian supervisory authority reiterated in its latest activity report. The good news is that the TIA does not need to be full-fledged as was required in pre-DPF times. Rather, the EU Commission has thankfully clarified that the DPF safeguards on the U.S. side also apply to any data transfers to the U.S., regardless of the transfer mechanism used. This means in practice that EU exporters can rely on the EU Commission's assessment of the legal situation in the U.S., omitting the complex analysis of U.S. laws. This makes life considerably easier not only for the TIA, but also because no supplemen-tary measures are required.