

*German Supervisory Authority
Publishes First Substantive Guidance
on International Data Transfers in the
Post Schrems 2.0 Era*

*Christian Schröder, Shannon Yavorsky, Dennis
Schmidt, and Yumiko Olsen*





Trust Anchor

German Supervisory Authority Publishes First Substantive Guidance on International Data Transfers in the Post Schrems 2.0 Era

Christian Schröder (<https://blogs.orrick.com/trustanchor/author/cschroeder/>), Shannon Yavorsky (<https://blogs.orrick.com/trustanchor/author/syavorsky/>), Dennis Schmidt (<https://blogs.orrick.com/trustanchor/author/dschmidt/>) and Yumiko Olsen (<https://blogs.orrick.com/trustanchor/author/yolsen/>)



On 16 July, 2020 the European Court of Justice (“**CJEU**”) published its decision invalidating the EU-U.S. Privacy Shield and setting out enhanced requirements for using the so-called Standard Contractual Clauses for Processors (Decision 2016/1250 – “**SCCs**”) (judgement C-311/18 – “**Schrems II**”). See our previous **blog** (<https://blogs.orrick.com/trustanchor/2020/07/16/privacy-shield-sunk-sccs-treading-water-what-can-companies-do-to-keep-their-head-above-water/>) on the Schrems II decision for further details. Shortly thereafter, the European Data Protection Board (“**EDPB**”) adopted FAQs (see our follow-up **blog** (<https://blogs.orrick.com/trustanchor/2020/07/29/how-to-comply-with-international-transfers-the-regulatory-guidance-overview-on-the-schrems-ii-decision/>) post), which mainly focused on how to

conduct the required risk assessment in connection with the SCCs.

Whereas the CJEU was very clear that companies need to act in order to remain in compliance with the GDPR’s requirements with respect to cross-border data transfer, companies found themselves scrambling to make sense of the rather abstract guidance provided by the CJEU and the EDPB.

On 24 August, the Data Protection Supervisory Authority for the State of Baden-Wuerttemberg (*Landesbeauftragter für Datenschutz und Informationsfreiheit Baden Württemberg*, “**Supervisory Authority**”), one of 17 German data protection supervisory authorities, issued more substantive guidance (“**Guidance**”) on how to conduct the necessary analysis and risk assessment. The Guidance is particularly noteworthy as it calls into question whether data transfers to the U.S. based on the SCCs can continue if they are not accompanied by additional measures such as encryption. In addition, the Supervisory Authority threatens companies with enforcement actions if they fail to take the required steps.

In this blog post, we summarize the Guidance, analyze the practicality of the recommendations and provide guidance on how companies should proceed.

What are the Key Features of the Guidance and What Should Companies Do?

- **Privacy Shield:** The Supervisory Authority indicates that it will not hesitate to issue fines against companies that still rely on the EU-U.S. Privacy Shield for data transfers to the U.S.

- If not already done, companies should immediately determine whether they or their vendors still rely on the Privacy Shield for transfers of personal data into the U.S. If so, companies should pivot to an alternate method of cross-border data transfer, such as the SCCs.
- **Data Transfers to the US:** The Supervisory Authority takes the view that, at least for data transfers to the U.S., the SCCs alone would not ensure an essentially equivalent level of data protection. As a result, either supplementary measures would be needed or data transfers would need to be limited to occasional transfers or to specific situations. According to the Guidance, such additional measures could include encryption, anonymization or pseudonymization of the personal data at issue. However, the Supervisory Authority appears to require that the encryption mechanism is one that cannot be decrypted by foreign intelligence services. Further, the Guidance indicates that, where possible, data should be pseudonymized in a way that only the company transferring the data to another country would be able to re-identify the relevant individual.
 - Companies should focus on applying state-of-the-art encryption mechanisms. However, given the technical know-how and capacities of most intelligence services, it remains questionable from a technical perspective whether an encryption mechanism actually exists that could withstand decryption efforts including brute-force attacks by intelligence services. Thus, companies should focus on using encryption mechanisms that make access to personal data considerably more difficult. We assume that state-of-the-art encryption mechanisms will still have a beneficial impact from a sanction risk perspective, provided the company has documented its efforts in this regard.
- **Consider Data Migration:** The Supervisory Authority suggests that companies should review every data transfer and determine with every service provider whether the data transfer remains justifiable. The Supervisory Authority recommends considering localizing the personal data in the EEA in order to avoid a transfer of data to third countries.
 - Companies should determine whether they can mitigate risks by using additional technical or contractual measures or assessing whether a data transfer is still justifiable without any further supplementary measures. If not, companies should check whether it is feasible to localize data in the EEA. While service providers may still have remote access to personal data located on servers in the EEA, the risks associated with mere remote access are lower than storing the data on servers located in a country outside the EEA.
- **Data Transfers to Other Third Countries:** The conditions imposed on continuing to rely on the SCCs do not apply only to data transfers to the U.S. but also to all other countries that do not provide an equivalent level of protection. Consequently, an assessment must be conducted, and measures taken (if necessary) in relation to all data transfers to countries located outside the EEA that do not have adequacy decisions.
 - Companies should assess where they are transferring personal data. On the basis of this assessment, companies should reach out to their contractual partners or service providers in the respective countries in order to understand the applicable legal framework.
- **Privilege for Group Internal Data Transfers?** The EDPB's **guideline (https://edpb.europa.eu/our-work-tools/our-documents/smjernice/guidelines-22018-derogations-article-49-under-regulation_en)**s on data transfers on the basis of Art. 49 continue to apply. While the EDPB emphasized in the FAQs that it takes the view that data transfers for the performance of a contract must be *occasional*, the Supervisory Authority suggests that Art. 49 GDPR could be appropriate for intra-group data transfers and individual contracts, i.e. also for *non-occasional* limited data transfers.

- Given the limited scope of Art. 49 GDPR (that the Supervisory Authority seems to endorse), this is a rather innovative approach and would certainly be helpful for intra-group data transfers. It remains to be seen in which cases such data transfers can actually be justified under Art 49 GDPR and further guidance in this regard is highly anticipated...
- **Suggested Contractual Improvements:** The Supervisory Authority suggests certain amendments to the SCCs to demonstrate the transferring parties' intentions to mitigate the risks associated with transfer of personal data. The Supervisory Authority in particular recommends modifying the applicability of Sec 4 lit. f, Sec. 5 lit. d (i) and Sec. 7 (1) of the SCCs to ensure that (i) data subjects will be informed of a transfer of their personal data to a third country, (ii) data subjects will be informed of any disclosure of such data to enforcement authorities (where this is prohibited by law the data importer consults with the supervisory authority in the EU), (iii) the data importer in the third country is obliged to take legal actions against such disclosure requests and personal data will only be disclosed upon final judgement; and (iv) disputes will only be referred to the courts in the member state in which the data exporter is established. In addition, the Supervisory Authority suggest implementing a clause on indemnification for breaches of the provisions set forth in the SCCs.
 - Companies should reach out to their service providers in third countries or their affiliates and suggest negotiating supplementary clauses to accompany the SCCs.
- **Measured Approach:** The Supervisory Authority indicates that it will in its assessment also take into account whether the transfer of personal data to a third country is actually necessary, i.e. it requires companies to assess whether reasonable alternative service providers exist in countries within the EEA or otherwise providing for an essentially equivalent level of data protection. The Supervisory Authority also states that it will prohibit transfers of data to service providers in third countries if the transferring company cannot demonstrate that the engagement of this particular service provider located in a third country is irreplaceable but that any such enforcement actions would be measured.
 - Companies should place a particular focus on the description of the services provided by their services providers located in third countries, e.g. in data processing agreements. Generic descriptions are likely to be challenged by the Supervisory Authority with the argument that equivalent service providers exist in the EEA so that it is important to document the uniqueness of the services provided. The Supervisory Authority did not clarify whether economic considerations will be taken into account when assessing the uniqueness of the services. It is questionable whether this view can be upheld as this severely limits the freedom to operate.
 - The fact that the Supervisory Authority notes that any of its enforcement actions will be measured and proportionate should be self-explanatory as this is a fundamental principle of European law. However, it is nevertheless a good sign that, unlike the CJEU, the authorities do not consider privacy rights to be absolute. The legal principle of proportionality of state actions will thus help companies to defend a continued transfer of data where the overall risks to the personal data seems limited and where clear economic needs/advantages speak in favor of a continued data transfer.