STATEMENT

Contribution of the German Association for the Digital Economy (BVDW) e.V. to the Consultation of the European Data Protection Board (EDPB) on its Recommendation 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data

10 December 2020

Contact:

Katharina Rieke
Bereichsleiterin Politik und Gesellschaft
T: +49 30 206 218 617
rieke@bvdw.org

Preliminary Remarks

The German Association for the Digital Economy (BVDW) e.V. has been representing digital business models since 1995. We incorporate the experience of our founding members from the online marketing industry as well as the global perspective of tech players from all over the world. More than 700 companies are now organized within BVDW which means that we cover the entire spectrum of the diverse digital ecosystem. Our positions represent the interests of the industry as a whole which makes BVDW a reliable partner for decision makers in Germany, Europe, and the world.

We thank the European Data Protection Board (EDPB) for opening up their Recommendation 1/2020 to a public consultation period and thereby giving us the chance to share our views on this crucial topic. We especially thank the Board for the prolongation of the consultation period (deadline 21. December), because this topic is key for the whole digital ecosystem and therefore a wide range of industries and companies. It is important to get as many meaningful contributions as possible and to use the momentum to establish a working system for our economy that is relying more than ever on data and the transfer of data in a globalized world.

3 KEY POINTS OF CRITICISM

- **The Recommendation does not provide enough added value as it does not increase legal certainty for companies. Concret practical supplementary measures with a contractual, technical or organisational nature are missing.**
- **It outlines a six-step procedure that is disproportionately burdensome on companies and especially SMEs.**
- **The Use Cases are not helpful enough as they do not fill gaps through supplementary measures.**

In detail

Overall approach

- The Recommendation aims to support companies in dealing with the consequences of the recent CJEU judgment C-311/18 (Schrems II).

- The consequences are well described and the questions raised in this Recommendation are crucial for companies to continue their daily business.

- All app. 700 members of BVDW deal with data on a daily basis and rely on the transfer of data in their business models. It is therefore key for them to have legal certainty to be able to continue their business.

- From our perspective the goal of the Recommendation is not achieved, because it does establish a six-step system, giving companies a procedure to follow, but it does not change the current situation for these companies as they are still required to assess their situation and the legal system of a third country themselves on a case-by-case basis and they fear the risk of a legal violation and possible fines because their assessment might have been wrong.

  The analysis of Step 3 "*Assess whether the Article 46 GDPR transfer tool you are relying on is effective in light of all circumstances of the transfer*" is entirely up to the companies. In practice this is a disproportionate burden on companies and it puts especially SMEs at a high disadvantage. The roadmap requires first of all a detailed analysis of the characteristics of every transfer, and then also an assessment of all applicable local laws (including complex surveillance laws) and how they impact on the requirements under EU law. This is a highly complex task that requires specialists, lawyers and resources that particularly SMEs do not have.

- Even though the Recommendation lists elements that should be considered when making this assessment, companies are still left alone with this decision and there is no level of legal certainty for them.

Lack of clarity

- The Recommendation does not provide full clarity which transfers are covered by it and which fall out of the scope because they are maybe not attributable to a controller or processor. For example, controllers or processors solely storing data in their systems within the EU/EWR are not "disclosing" data to third parties that gain unauthorized access to such data (even if the contracting party is registered in a third country) nor should transfers be covered that are attributable to the data subjects themselves. The Recommendation should hence be reviewed with the aim to clarify which transfers are covered.

- Additionally, the Recommendation does not distinguish between different categories of risk. For example, not any kind of data has the same risk. Health data affects the rights and freedoms of natural persons much more and is hence more sensitive than other data. This risk-based approach that also takes the factor of likelihood in the sense of probability into account, is well known and applied within the GDPR system, so it should also be applied here. Looking at different categories of risk would additionally help companies with better focusing their efforts.

- Another example close to the daily business of our members is pseudonymized data. A majority of our members transfer pseudonymized data for which the risk is much lower. In its Use Case 2 "transfer of pseudonymised data", the EDPB considers generally pseudonymisation performed as an effective supplementary measure. However, under the conditions of the Use Case described by the Board, there is doubt, whether personal data is transferred to the third country in question or not. What is particularly problematic, however, is that the use case cannot be implemented in practice in this way and misses the reality.

Use Cases

- BVDW is of the opinion that the presented Use Cases are not very helpful. The EDPB states that in cases *"where the law or practice of a third country impinges on the effectiveness of the appropriate safeguards contained in the Article 46 GDPR transfer tools, the Court still leaves open the possibility for exporters to implement supplementary measures that fill these gaps in the protection and bring it up to the level required by EU law."* However, the Use Cases do not achieve the goal to provide practice-oriented examples of supplementary or additional measures and are therefore not actually filling any gap.

- Use Cases 6 and 7 are even cases where a transfer in violation of the GDPR is already assumed, and no supplementary measures are suggested. This also takes away a lot of room for maneuver for the industry.

Conclusion

BVDW therefore sees the need to adapt this Recommendation to ensure a higher level of support and legal certainty for companies. This would be achieved by the following elements:

- Developing Use Cases that show practice-oriented supplementary measures
- Further in-depth guidance by the EDPB on Step 3 and Step 4
- Further guidance not only on SCCs but also on the other transfer tools of Article 46 GDPR
- A department within the EDPB that is available for support and questions on this matter

Furthermore, a harmonized approach in the form of a Privacy Shield 2.0 or SCCs that work for everyone would be the most beneficial way to give companies the security they need. When thinking about a new Privacy Shield type of agreement with the US, it would be important to ensure that it is future proof and will last for many years to come.