Data transfer to third countries – moderate implementation of the Schrems II ruling of the ECJ
The associations supporting the initiative represent all companies in the German economy. They are concerned that the consequences of the Schrems II ruling of the European Court of Justice (ECJ) will have a massive negative impact on the German economy and argue for moderate implementation. This is all the more urgent as the validity of the EU standard data protection clauses has recently also been questioned by some data protection supervisory authorities in the EU.

Global interconnection of the German economy
German companies are connected around the world. The digitization of the economy makes a significant contribution to this. Data transfers to countries outside the EU not only play a role for international corporations and global sales markets. Smaller companies are also increasingly storing data in the cloud, using software from US providers and using social networks and web conference systems from international providers for communication. Support services are often also offered from Asia. If companies outsource tasks to external service providers in third countries, it is often necessary to transfer employee data in order to fulfill their tasks.

The judgment
With its judgment of July 16, 2020 (Case C-311/18, Schrems II), the ECJ declared the EU Commission's adequacy decision on the transfer of personal data to the USA (EU-US Privacy Shield) invalid.

The ECJ does not consider the level of the data protection in the USA to be adequate according to Art. 45 GDPR. It held that there is a lack of suitable guarantees, enforceable rights and effective legal remedies against requests by intelligence services to surrender personal data of EU citizens that are processed in or transmitted to the USA. The ombudsman provided for in the Privacy Shield does not offer sufficient protection against the intelligence services according to the Court.

The ECJ also had to rule on the EU standard data protection clauses established by the EU Commission in accordance with Art. 46 Para. 2 lit. c GDPR. Although the Court still considers them a valid basis for data transfer to third countries, the respective controller must check whether the use of these clauses can actually create an equivalent level of data protection for the recipient. If this is not the case, he or she will have to provide additional measures or safeguards. If this cannot be ensured, the data transmission shall be stopped and the data retrieved.

The consequences
As the ECJ was unable to determine an adequate level of data protection in the USA due to surveillance authorities of U.S. law enforcement and intelligence agencies and the lack of legal remedies, the continued use of the EU standard data protection clauses established by the EU Commission could also be called into question. This puts companies - and possibly the public sector as well - in a dilemma, although constant data transfer to the USA is common practice. In addition, the companies now have to negotiate with their business partners on a case-by-case basis and can no longer make use of the standard data protection clauses as suitable guarantees.

In this way, for important countries like the USA, the responsibility for ensuring an adequate level of data protection for the processing of personal data is unilaterally shifted to the controller in the EU. However, it is not clear what additional measures or safeguards must entail and when they are sufficient in terms of content. As a result, there is a significant legal risk for companies – either controllers or processors who are dependent on data transfer to the USA. The same applies to data transmission to other third countries for which there are no adequacy decisions (e.g. India). The alternative of binding corporate rules does not exist, especially for SMEs. In addition, due to the approval requirements, such rules require a considerable lead time before they are valid, and in the opinion of the European Data Protection Board they are subject to the same requirements as the standard data protection clauses.

Proposals of the German economy:
In order to eliminate the existing legal uncertainty and to prevent data processing from being significantly blocked in the German economy, we recommend:

- The EU Commission, with the involvement of the European Data Protection Board (EDPB), should negotiate an effective follow-up instrument to the Privacy Shield with the US authorities as quickly as possible and improve the EU standard data protection clauses. An EU-wide uniform solution is required, especially in terms of the GDPR.

- The EU Commission and the data protection supervisory authorities should promptly publish uniform information on the level of data protection in third countries so that not every authority and every company has to carry out the check itself.

- The data protection supervisory authorities should also formulate uniform EU criteria that give companies indications for a permissible procedure when transferring data to third countries. Mentioning possible and sufficient protective measures for typical processing cases would be particularly helpful for small and medium-sized companies. A risk-based approach would be imaginable that enables data transfers with weaker protective measures if the risks to the rights and freedoms of the data subjects do not appear high. In doing so, the type of data, the type and period of access, the purpose and circumstances of the processing as well as existing technical and organizational measures (e.g. use of pseudonyms) should be taken into account.

- The data transfer to third countries on the basis of standard data protection clauses and binding corporate rules, which is expressly provided for in Art. 46, 47 GDPR, must not be ruled out in practice and must also be possible in the future.

- The exemptions provided for in Art. 49 DSGVO for data transfers to third countries must not be restricted by the EDPB guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679.

- If a data transfer to the USA is not based exclusively on the Privacy Shield, - contrary to the announcement of some data protection supervisory authorities - sanctions must be suspended until legal clarity has been created.

- The renewed legal uncertainty that has arisen should be used as an opportunity to adapt the sometimes extremely narrow and internationally not consistently accepted standards of the GDPR.

In view of the considerable legal uncertainty, we ask you to act quickly and are available for a constructive exchange on practical implementation options.