The associations supporting this initiative represent companies from all sectors of the German economy. They already called for a **measured implementation of the Schrems II ruling of the European Court of Justice (CJEU)** and for a political solution in an open letter last September.

The consequences of the CJEU's Schrems II ruling continue to have a massive impact on the German economy which heavily depends on global cooperation. Legal uncertainties regarding international data transfers are hampering trade, data exchange and economic cooperation, which are of the utmost importance for maintaining and rebuilding the economy, which is currently under particular strain. The consequences of the Schrems II ruling are also being felt by small and medium-sized enterprises that store data in the cloud, use software from U.S. or other globally active providers, have a presence on social networks and use web conferencing systems from international providers.

Globally networked economic relationships are of fundamental importance for people and companies in Germany and Europe. For this purpose, the flow of personal data between Europe and the U.S. as well as third countries in Asia and South America is essential and without alternative.

With its decision of July 16, 2020 (Case C-311/18 - Schrems II / Privacy Shield), the CJEU invalidated a key legal basis for data transfers between the EU and the U.S. and established additional requirements for the use of the EU standard contractual clauses. The resulting legal uncertainty, which is still ongoing, affects large corporations as well as SMEs and start-ups from all sectors of the economy. It leads to massive competitive disadvantages for German and European companies in a globalized economy. The effects will also lead to less development and innovation regarding certain sectors. The guidance provided by the European Data Protection Board on the implementation of the CJEU ruling may provide some assistance in certain constellations, but it does not eliminate the dilemma. Companies continue to face a great deal of uncertainty with regard to global contracts and the expansion of business activities outside the EU until there is clarity about the future of the data transfer framework. This is also an extremely critical situation for the further development of both the analogue and digital economies and innovations in Germany and the EU if international data flows are cut off. The situation is further exacerbated for companies in Germany by the fact that the state data protection authorities are currently preparing a concerted implementation and enforcement of the CJEU ruling.

Of particular importance is maintaining cooperation and free, legally secure data transfer between the EU and the U.S. due to the trade relations that have been established for decades. Germany, the EU and the USA share many

common values, comparable fundamental rights and principles of the rule of law. There is consensus among Germany, the EU and the U.S. that the protection of privacy and the security of personal data must be a top priority. This makes it all the more important that the U.S. and the EU find a political solution that should serve as a blueprint for global trade. Political representatives in the U.S. and the EU must now quickly send a signal in order to jointly find a reliable, legally secure data space that ensures the opening of transatlantic data traffic while respecting fundamental rights.

To date, no concrete solution worthy of discussion has been proposed by those responsible, so there is still an urgent need for action. A lasting and fundamental solution can only be achieved at the political level. It is encouraging that in March 2021, the EU Commission and the U.S. administration began talks for the amendment of the EU-US Privacy Shield.

We now call for **increased efforts by both the German government and the European Commission** to quickly bring about legal certainty for companies as well as **a long-term political solution**.

In the meantime, **pragmatic solutions – also with regard to data transfers to other third countries** – must be found. After all, even if international data traffic only temporarily collapses, this will cause considerable conversion costs and setbacks for the European economy that are difficult to make up.

For this reason, all interpretation by the supervisory authorities should strictly follow the GDPR and companies should be provided with practicable guidelines:

- The risk-based approach of the GDPR should be taken into account for data transfers to third countries. Following the GDPR´s rules, additional safeguards should only be required as are proportionate to the nature of the data transferred, the scope and circumstances of their processing, and the likelihood and severity of the risk to data subjects.

- The exceptions provided for in Article 49 GDPR should not be interpreted in a restrictive manner beyond their wording. In particular, the GDPR allows data transfers to third countries on the basis of voluntary informed consent. This is in line with the right to informational self-determination and Article 8 of the EU Charter of Fundamental Rights. It is also important to note that certain data transfers to third countries may also serve to fulfil contractual obligations to customers (e.g., in global payment transactions).

- The EU Commission and the supervisory authorities should promptly issue uniform information on the level of data protection in third countries so that each authority and each company does not have to conduct the examination itself.