Centrum für Europäische Politik
FREIBURG | BERLIN

cep**Study** – Key Points

26 January 2021

Illegality of data transfers to the USA

The “Schrems II” ruling of the European Court of Justice and its consequences

Anja Hoffmann

Following the "Schrems II" ruling of the European Court of Justice, transfers of personal data to the USA may no longer be based on the "Privacy Shield" decision because the USA does not offer sufficient data protection. Currently, therefore, data transfers are mainly based on standard contractual clauses, the use of which remains lawful, in principle.

- Standard contractual clauses and Binding Corporate Rules cannot, however, be used as a basis for data transfers to the USA if the data recipients are subject to US surveillance laws and have access to the data content in plaintext.
- In such cases, even supplementary data protection measures cannot effectively prevent access by the US authorities.
- Transfers to US-based cloud services and transfers to the US within corporate groups are therefore illegal in these cases. The data exporter – or supervisory authority – must stop the data transfer.
- Neither a reformed “Privacy Shield” nor the amended standard contractual clauses proposed by the EU Commission in November 2020 will change this situation as long as the USA does nothing to limit its surveillance laws to what is permissible under EU law or fails to grant EU citizens effective remedies.
- The same applies to data transfers to other third countries insofar as their surveillance laws are incompatible with EU data protection standards. This must be examined in each individual case.

Key Points

On the ECJ ruling in the case of “Schrems II”

- Transfers of personal data from the EU to the USA may no longer be based on the EU Commission‘s "Privacy Shield" decision. The European Court of Justice (ECJ) has rightly invalidated this decision in the “Schrems II” ruling because the “Privacy Shield” does not offer an equivalent level of data protection to that of the EU.
- Data transfers to a third country on the basis of standard data protection clauses (SDPC) – these are data protection model clauses adopted by the EU Commission which are contractually agreed between the data exporter and the data recipient – remain lawful, in principle. However, data exporters and recipients must check whether the law of the third country and the SDPC together ensure a level of protection for the data that is essentially equivalent to that ensured within the EU, and that the data subjects whose data are transferred have enforceable rights and effective remedies.

On implementation of the "Schrems II" ruling

- Following the ruling, the European Data Protection Board (EDPB) has published two sets of draft recommendations. According to these recommendations, the level of protection in the third country must be assessed in light of all circumstances of the specific data transfer – inter alia the categories and format of the transferred data –, while the likelihood of access to the data by public authorities should not be taken into account.
- Furthermore, according to the SDPC, the data exporter and the data recipient must satisfy themselves that the law in the third country also allows the data recipient to comply with the SDPC. Data transfers to recipients on whom the law of the third country imposes obligations which are contrary to the SDPC and undermine their guarantee are particularly problematic.
- According to the EDPB, the data recipient’s obligation to disclose or grant access to data to authorities in the third country does not prevent compliance with the SDPC if the third country meets the requirements of the "European Essential Guarantees" with regard to its surveillance measures.
- Surveillance measures meet the EDPB’s "European Essential Guarantees" if they are based on clear rules for data processing, interference is necessary and proportionate, and independent oversight and effective legal remedies exist in the third country.
- If the surveillance measures do not meet the Guarantees – which the US surveillance laws do not – there is no essentially equivalent level of protection. In this case, the SDPC alone do not provide sufficient safeguards; the data exporter must therefore add supplementary data protection measures.
- There is legal uncertainty as to what supplementary measures the data exporter must take to ensure an equivalent level of protection. The supervisory authorities propose technical measures such as anonymisation, encryption, pseudonymisation or splitting of data, supplementary contractual clauses and organisational measures.
- Stricter contractual obligations, e.g. duties to provide information on or to challenge data access requests, and organisational measures such as internal guidelines, increase protection but are not sufficient and must be supplemented by technical measures. Even stricter contractual obligations cannot bind the authorities in the third country or create effective legal remedies for EU citizens.
- At best, technical measures can, in the EDPB's view, only effectively prevent disproportionate access by public authorities if even the data recipient is unable to decrypt, de-pseudonymise or reconstruct the data. This only applies in a limited number of use cases, such as when data is stored in a third country solely for backup purposes.

- If the data recipient has or needs access to the data in plaintext in order to process it, even technical measures cannot effectively prevent access to the data by the authorities. If the recipient is in possession of the key, he could be obliged to hand it over to the authorities. The "backdoors" in encryption software currently under discussion would also undermine protection.
- If the data exporter cannot – through additional measures – guarantee a data protection level equivalent to that within the EU, he – or failing that, the supervisory authority – must stop the data transfer. In the case of transfers to the USA, however, no measures are apparent that could effectively prevent access to the data by the authorities under US surveillance laws, unless the recipient of the data is also barred from accessing it.
- For the reasons outlined above, the amended SDPC proposed by the Commission in November 2020 can also only provide equivalent data protection in combination with technical measures. To avoid even more uncertainty, the new SDPC should be more closely aligned with the EDPB recommendations.

Conclusions for transfers of personal data to the USA

- All data transfers to recipients in the USA who are subject to US surveillance laws and who have access to the data in plaintext are therefore currently unlawful. Among others, transfers to providers of cloud services and transfers within corporate groups for the provision of personnel services are affected.
- EU data protection authorities should provide guidance on the interpretation of which data recipients are covered by US surveillance laws and which transfers therefore require critical assessment.
- As long as the US does nothing to limit its surveillance laws to what is necessary and fails to grant EU citizens effective remedies, neither enhanced SDPC nor a new, "improved" Privacy Shield will help.

Consequences for other transfer instruments and data transfers to other third countries

- The ECJ's findings on the SDPC can also be applied to other transfer instruments such as Binding Corporate Rules (BCR). Their use therefore involves comparable risks for data transfers to the USA if the recipients are subject to US surveillance laws.
- Surveillance laws that conflict with the SDPC may also exist in other third countries. Data exporters who intend to transfer data to other third countries for which there is no adequacy decision must therefore also check the level of protection and supplement the SDPC if necessary. Data transfers to the United Kingdom remain permissible, at least for a limited period.
- The EU Commission must critically review existing adequacy decisions relating to other third countries and check whether they (still) meet the requirements set by the ECJ.

Conclusion

- The legally safest solution is to refrain from the aforementioned data transfers to third countries, to store the data in the EU in such a way that US companies or their subsidiaries have no control over it, and only use European providers who do the same.
- The high data protection requirements in the EU clash with current transfer practices. Data exporters who do not stop illegal data transfers risk high fines. Even the draft recommendations of the EDSA and the EU Commission’s amended SDPC at best allow in a limited number of use cases for possible solutions to this dilemma which are both legally sound and at the same time practicable.
- The "Schrems II" ruling offers the chance to strengthen high-quality and secure services (e.g. clouds) in the EU. Only then will switching to EU service providers be an alternative in the long term. The creation of Gaia-X, the first European cloud, may be a step in the right direction.

The full version of the cep**Study** has been published in German. Please follow this link:

cep**Studie**: Unzulässigkeit der Datenübermittlung in die USA

Table of Contents

Author:

Dr. Anja Hoffmann LL.M. Eur

hoffmann@cep.eu

Centrum für Europäische Politik FREIBURG | BERLIN

Kaiser-Joseph-Straße 266 | D-79098 Freiburg

Schiffbauerdamm 40 Raum 4315 | D-10117 Berlin

Tel. + 49 761 38693-0

The **Centrum für Europäische Politik** FREIBURG | BERLIN, the **Centre de Politique Européenne** PARIS, and the **Centro Politiche Europee** ROMA form the **Centres for European Policy Network** FREIBURG | BERLIN | PARIS | ROMA.

The cep institutes are specialised in the analysis and evaluation of European Integration Policy. They publish their scientific work independently of any vested interest, in favour of a European Union that respects the Rule of Law and the principles of the social market economy.