# PRIVACY LAW

## CJEU on international data transfers: EU-US Privacy Shield no more, SCCs in doubt

With its decision of 16 July 2020 in case C-311/18 ("Schrems II decision"), the Court of Justice of the European Union (CJEU) has invalidated the EU-US Privacy Shield mechanism widely used for transferring personal data from the EU to the USA.

More importantly, the Court cast aspersions on the use of Standard Contractual Clauses ("SCCs") as a mechanism for international data transfers, though it did not declare these to be invalid *per se*.

This decision will have an enormous impact on both transatlantic and global data transfers. Data exporters within the EU will need to take urgent action to ensure compliance.

### WHAT HAPPENED?

Austrian lawyer and activist, Maximillian Schrems, complained to the Irish Data Protection Commissioner about the transfer of his personal data from Facebook Ireland to Facebook Inc., located in the USA. He argued that the requirement to grant access to the personal data to US authorities, such as the FBI and the NSA, and the use of the personal data by those authorities in mass surveillance programmes meant that the transfer of his personal data from the EU to the USA would breach his rights under the Charter of Fundamental Rights of the European Union.

### EU-US PRIVACY SHIELD INVALID

In 2015, the CJEU declared the Safe Harbor Privacy Principles, the mechanism for ensuring adequacy of data protection when transferring personal data from the EU to the USA, to be invalid. In response, the EU and the USA negotiated the EU-US Privacy Shield in 2016, which foresaw US companies being able to self-certify compliance with the standards of the EU-US Privacy Shield, those standards being higher than those to which they are subject by virtue of US domestic law. The US government also provided guarantees and made assurances regarding limitations on access to personal data by US agencies and guaranteed that it would ensure compliance by companies with their obligations under the EU-US Privacy Shield. The EU Commission adopted an adequacy decision on the basis of the EU-US Privacy Shield framework, enabling personal data to flow from EU data exporters to US data importers which had self-certified compliance with the EU-US Privacy Shield obligations.

According to the CJEU, despite the additional protections foreseen by the EU-US Privacy Shield, the comprehensive mass surveillance activities undertaken by (amongst others) the NSA and the FBI have continued. The NSA is permitted to access, collect and retain personal data "in transit" to the United States before it reaches the USA by accessing underwater cables, avoiding the applicability of the US Foreign Intelligence Surveillance Act – and thereby the applicability of those safeguards that do exist under US domestic law. The CJEU considers European data subjects to be largely left without any effective and enforceable rights against US authorities and also unable to access any effective remedy before a court or tribunal with respect to many mass surveillance programmes.

Therefore, it comes as no surprise that the CJEU determined that the EU-US Privacy Shield is incompatible with Article 45(1) GDPR and declared it invalid.

### SCCS: "SIGN AND FORGET" APPROACH IS DEAD!

Pivotally, the decision of the CJEU also focussed on the validity of the SCCs as a mechanism for ensuring adequacy of data protection in a third country. The SCCs are frequently concluded between a data exporter in the EU and a data importer in a third country to ensure an appropriate safeguard pursuant to Article 46 GDPR. Whilst the Court did not go so far as to invalidate these as a method for ensuring data adequacy *per se*, it dismissed the notion that a data exporter simply agreeing SCCs with a data importer in a third country was sufficient to guarantee an adequate level of data protection.

The CJEU held that, when using SCCs to ensure appropriate safeguards for data transfers to third countries, the data exporter must verify, on a case-by-case basis, whether the law of the third country of destination ensures adequate protection of the personal data transferred. Where this cannot be verified, adequate protection can be achieved through the adoption of "supplementary measures" to ensure compliance with the level of protection.

Where data exporters are unable to take adequate supplementary measures to guarantee the protection, they are required to suspend or terminate the transfer of personal data to the third

country concerned. Although this leaves SCCs as a transfer mechanism intact, it places the onus on the data exporters to ensure that the third countries to which they transfer data have an adequate level of data protection.

### BINDING CORPORATE RULES AND CONSENT

Presently, Binding Corporate Rules (BCR) could serve as an alternative to transferring personal data to the USA. However, BCR are not suitable for many data exporters. Additionally, although BCR were not the subject of the decision in question, many of the same considerations will apply to BCR as applied to SCCs – namely the lack of enforceable rights and remedies and being subject to mass surveillance incompatible with EU law.

Transfers could also occur on the basis of the derogation under Article 49 GDPR (e.g. explicit consent of the data subject). However, the scope of Article 49 GDPR is greatly limited and it cannot be employed where the transfer is repetitive or concerns more than a limited number of data subjects.

### WHAT SHOULD BUSINESSES DO NOW?

The next steps businesses should take are as follows:

- Data exporters of all sizes and types need to urgently review their data flows and their data transfer mechanisms. This applies for data transfers not only to the USA, but to all countries with extensive surveillance programmes and a lack of rights and remedies for data subjects.

- "Indirect data export" via a partnering EU entity to the USA must be reviewed as well, in particular where the controller contracts with an EU service provider which concludes SCCs as a proxy between the controller and a third party in the USA.

- Where data transfers are exclusively based on the EU-US Privacy Shield, and where the data cannot be relocated to the EU, businesses might consider entering into SCCs as a "quick fix", bearing in mind that this will most likely not be considered to be sufficient. "Supplementary measures" will have to be taken. As a preliminary measure, guarantees exceeding those foreseen under the EU-US Privacy Shield could be explored as an option. The era of signing and forgetting SCCs ceased on 16 July 2020 with the Schrems II decision.

- Data exporters should contact data importers and explicitly ask whether the data importers consider themselves as falling under the scope of US surveillance laws and which additional measures these data importers are prepared to put in place to guarantee an equivalent level of data protection.

- Data controllers need to document their risk analysis to demonstrate compliance with the requirements for transfer of personal data to third countries (see Articles 44 et seq. GDPR).

- Upcoming statements from the Data Protection Authorities as well as from the European Commission might give clearer guidance regarding such supplementary measures. The European Data Protection Board has published FAQ pertaining to the decision. These, however, leave the question unanswered of which particular legal, technical or organisational "supplementary measures" businesses may take when using SCCs or BCR. The European Commission announced at the beginning of July 2020 that it had begun conducting "preparatory work" for the eventuality that the CJEU would invalidate the EU-US Privacy Shield.

It is not yet clear how, in particular how fast, data protection authorities across the EU will sanction data flows to the USA which are (exclusively) based on the invalid EU-US Privacy Shield. The data protection authority in Berlin (*Berliner Beauftragte für Datenschutz und Informationsfreiheit*) has, however, already announced that it will prohibit data transfers to the USA and has encouraged businesses to switch immediately to service providers in the EU or in a country with an adequate level of data protection.

Therefore, it is vital that worldwide data flows across entire organisations are carefully assessed, scrutinised and adjusted accordingly and that this process is comprehensively documented.

If you have any questions, please address the BEITEN BURKHARDT lawyer of your choice or contact the BEITEN BURKHARDT Privacy Team directly:


### MUNICH

**Dr Axel von Walter**
Lawyer | CIPP/E | CIPM | Licensed Specialist for Copyright and Media Law | Licensed Specialist for Information Technology Law
Axel.Walter@bblaw.com
Tel.: +49 89 35065-1321

**Dr Johannes Baumann**
Lawyer
Johannes.Baumann@bblaw.com
Tel.: +49 89 35065-1307

**Gudrun Hausner**
Lawyer
Gudrun.Hausner@bblaw.com
Tel.: +49 89 35065-1307

**Laureen Lee**
Lawyer | LL.M.
Laureen.Lee@bblaw.com
Tel.: +49 89 35065-1307

### FRANKFURT AM MAIN

**Dr Andreas Lober**
Lawyer
Andreas.Lober@bblaw.com
Tel.: +49 69 756095-582

**Peter Tzschentke**
Lawyer
Peter.Tzschentke@bblaw.com
Tel.: +49 69 756095-582

**Susanne Klein**
Lawyer | LL.M.
Licensed Specialist for Information Technology Law
Susanne.Klein@bblaw.com
Tel.: +49 69 756095-582

**Lennart Kriebel**
Lawyer
Lennart.Kriebel@bblaw.com
Tel.: +49 69 756095-477

### BERLIN

**Dr Matthias Schote**
Lawyer | Licensed Specialist for Copyright and Media Law
Matthias.Schote@bblaw.com
Tel.: +49 30 26471-280

### DUSSELDORF

**Mathias Zimmer-Goertz**
Lawyer
Mathias.Zimmer-Goertz@bblaw.com
Tel.: +49 211 518989-144


## Imprint


This publication is issued by
**BEITEN BURKHARDT**
Rechtsanwaltsgesellschaft mbH
Ganghoferstrasse 33 | D-80339 Munich
Registered under HR B 155350 at the Regional Court Munich/VAT Reg. No.: DE811218811

For more information see:
https://www.beiten-burkhardt.com/en/imprint

**EDITOR IN CHARGE**
Dr Axel von Walter | Lawyer | Partner




**PLEASE NOTE**
This publication cannot replace consultation with a trained legal professional.

If you no longer wish to receive this newsletter, you can unsubscribe at any time by e-mail (please send an e-mail with the heading “Unsubscribe” to newsletter@bblaw.com) or any other declaration made to BEITEN BURKHARDT.