TaylorWessing

First guidance for action following the CJEU judgment „Schrems II“

29 July 2020

The first statements by data protection supervisory authorities on the Court of Justice of the European Union's (CJEU) Schrems II judgment have now been published. However, there is still considerable uncertainty over how to deal with data transfers to third countries that do not provide an adequate level of data protection.

If your company is affected, you should proactively review your data transfers to third countries by following the steps outlined below (measures taken in this context should be documented for verification purposes).

1

Find out which US data importers rely on the EU-US Privacy Shield

Examine which of your US data importers rely on the invalidated EU-US Privacy Shield. Essentially, you will need to look at the commissioned data processing agreements pursuant to Art. 28 GDPR with the corresponding contractual partners (ie data processors pursuant to Art. 4 no. 8 GDPR). It is also important to bear in mind that the processing of personal data between two data controllers (Art. 4 no. 7 GDPR) can be affected as well.

Furthermore, you should determine whether your data processors based in Germany, the EU and the EEA have engaged sub-data processors in the US. As part of this, consider whether these sub-data processors rely on the EU-US Privacy Shield.

2

Determine which of your US data importers are subject to other guarantees

Identify which of your US data importers – ie data processors and data controllers – undertake data transfers based on another guarantee under Art. 46 GDPR (eg EU Standard Contractual Clauses and Binding Corporate Rules).

3

Contact US data importers for further clarification

You should contact those US data importers identified under the first two steps and ask them to explain the extent to which US authorities can access the personal data transferred.

In particular, your US data importers should clarify whether they fall under the regulations discussed by the CJEU – ie 50 US Code § 1881a (Section 702 of the US Foreign Intelligence Surveillance Act) – or whether they make personal data available to US authorities under Executive Order 12.333 or other US regulations with comparable objectives (eg the US Cloud Act).

Depending on the responses you receive, you then need to decide whether

- the data transfer can be maintained in its current form;
- data transfers can be secured by additional safeguards (these are likely to be technical measures, such as effective encryption as opposed to merely contractual arrangements);

  or
- the personal data involved needs to be retrieved.

Ultimately, though, if the EU-US Privacy Shield has been the sole basis for your data transfers to date, switching to other appropriate safeguards in accordance with Art. 46 GDPR is mandatory.

REMEMBER:

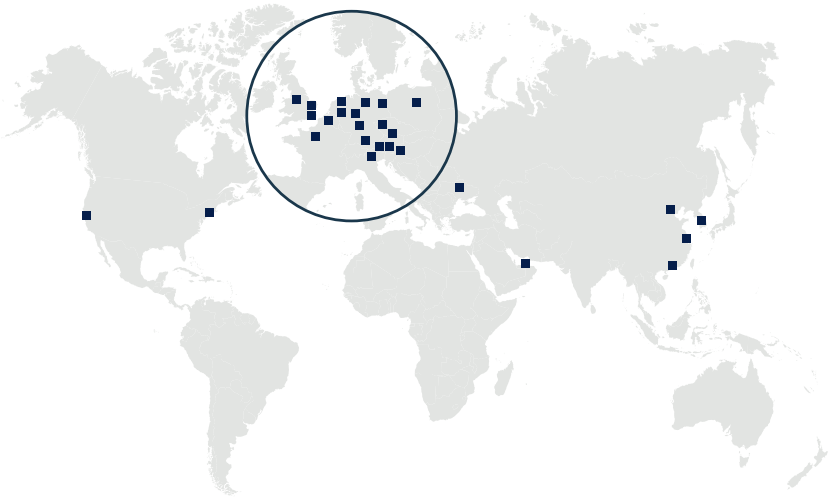
Check your data protection levels on a country-by-country basis

The CJEU (in its Schrems II judgment), the European Data Protection Board (in its FAQ published on 23 July 2020) and the German Datenschutzkonferenz (in its press release from 28 July 2020) have all clearly stated that data exporters need to check the level of data protection in the recipient country on a case-by-case basis and (if necessary) provide supplementary safeguards. This requirement is not limited to the US, but applies to all third countries, including India, China and (from 01 January 2021) the UK.

Do not delay, act today

As the data protection supervisory authorities have repeatedly made it clear that there is no transitional period, you should implement the three steps outlined above as soon as possible. Please contact a member of our Data Protection and Cyber team if you need further guidance regarding next steps or anything else covered in this article.

Find your **contact person** for data protection at Taylor Wessing and feel free to contact us at any time.



1000+ lawyers
300+ partners
28 offices
16 jurisdictions