AUSTRIA

Need for action regarding data transfers in third countries – EU-US Privacy Shield declared invalid by the ECJ

The European Court of Justice (ECJ) declared the EU-US Privacy Shield invalid and makes far-reaching requirements for data transfers in third countries.

In the case Data Protection Commissioner (Ireland) v. Schrems, Facebook Ireland (Case C-311/18; "Schrems II") the ECJ ruled on 16 July 2020 that

- the EU-US Privacy Shield is invalid with immediate effect and
- EU standard contract clauses (SCCs) are valid, but it must also be assessed on a case-by-case basis whether adequate and enforceable rights and effective remedies for data subjects actually exist in the third country.

The EU-US Privacy Shield is a decision of the EU Commission based on an agreement with the US. Key elements were, on the one hand, assurances from the US government and, on the other hand, data protection principles that US companies must comply with. US companies were able to register under the data protection shield and were thus considered to have an equivalent level of data protection, so that no further measures were necessary.

Who is affected?

All companies which transfer data to the USA are directly affected. Even if the data is transferred to an EU cloud of a US provider (e.g., Microsoft or Amazon), this usually also includes a transfer to the USA because US employees have access to the data for administration, provision of services, etc. However, also all others are also affected who transfer data to other third countries or use standard contract clauses.

What are the requirements for data transfers to third countries?

In general, a data transfer is only permissible if, among others, an adequate level of data protection exists in the recipient country. This is guaranteed within the EU and the EEA. For all other countries (so-called third countries) an adequate level of data protection must be guaranteed. This is done by:

- Adequacy decision of the EU Commission (currently for Switzerland, Canada, Argentina, Guernsey and the Isle of Man),
- Binding Corporate Rules (BCR), i.e., binding corporate or group-internal data protection regulations that have been approved by a data protection authority, or
- Standard Contract Clauses (SCC), i.e., model contracts by the EU-Commission which are concluded between companies and data recipients in third countries.

However, SCC and BCR are no longer sufficient on their own following the ECJ ruling. Also, the level of data protection in the third country must be examined and, if necessary, additional measures must be taken to ensure it.

What are the data protection authorities doing?

In addition to the wide variety of opinions issued by data protection authorities, there is also a first reaction from

Author:

Mag. Ingo Braun

✉ ingo.braun@benn-ibler.com
☎ +43 1 531 55 700

Benn-Ibler Rechtsanwälte GmbH
Tuchlauben 8, A-1010 Vienna

the European Data Protection Board (EDPB). It is strict but specific.

- There is no grace period.
- Data transfers to the US under Privacy Shield has to be stopped.
- Prior to any data transfer to the US on the basis of SCC or BCRs, it must be carefully examined whether an adequate level of data protection can be guaranteed, taking into account all circumstances and additional measures taken.
- If an adequate level of data protection cannot be ensured, the data transfer must be stopped. Otherwise, the company must inform the relevant data protection authority.

EDPB has announced to provide further information on the additional measures to be taken to ensure an adequate level of data protection.

What needs to be done?

The greatest need for action exists for companies with data transfers to the US. However, almost all data transfers to third countries are affected. The proposals published so far range from wait and see to full compliance with EDPB requirements.

While there is still legal uncertainty at present, the following steps can be taken:

- First of all, all data transfers and the data transferred should be identified and in each case the associated risk should be assessed.
- If data is transferred to the USA, possible solutions should be sought immediately. For example, switching to EU clouds (without access from the US for maintenance, etc.)
- The level of data protection in third countries should be analysed. For this purpose, it is possible to inquire with the contractual partner in the third country whether they are subject to the monitoring laws mentioned by the ECJ (i.e., Section 702 FISA and EO 12333).
- Additional measures can be considered. For example, a strong encryption of the data could be implemented. However, other legal, technical and organisational measures may also be appropriate.
- Watch out for further guidance by the relevant data protection authority and EDPB.
- Data Protection Officers will have to inform management about the consequences of the ECJ ruling and the data processing operations affected in the company. Ultimately, every change will also lead to costs.

Since an immediate change or termination of data transfers to third countries is impossible for most companies, it is at least possible to demonstrate rapid action in the event of enquiries from the data protection authority. Even if no penalties can be avoided, this would at least need to be considered to the benefit of the company.

Author:

Mag. Ingo Braun

✉ ingo.braun@benn-ibler.com
☎ +43 1 531 55 700

Benn-Ibler Rechtsanwälte GmbH
Tuchlauben 8, A-1010 Vienna