COSMOS
Navigate the Compliance Universe

CEP Magazine - March 2021
Post-Schrems II EU guidance on data transfer mechanisms-a critique

By Robert Bond

Robert Bond (robert.bond@bristows.com) is Senior Counsel & Notary Public at Bristows LLP in London, UK.

The Court of Justice of the European Union (CJEU) ruling on the validity of the European Commission's standard contractual clauses (SCCs) for international data transfers from the European Union (EU) to third countries was announced on July 16, 2020.[1]

The CJEU declared that the European Commission's decision approving the SCCs was still valid. However, this does not automatically mean that all data transfers made under the SCCs are valid, as the decision emphasizes the obligations on controllers to suspend transfers if the clauses can't be complied with (e.g., government surveillance programs). The CJEU also ruled that the Privacy Shield was invalid.

The key points of the decision include the following:

- Data subjects whose data are transferred to a third country must be given a level of protection essentially equivalent to that guaranteed under the General Data Protection Regulation (GDPR), read in the light of the EU Charter of Fundamental Rights.
- US government surveillance programs and the limitations they are subject to do not meet the requirements of proportionality under EU law and do not grant data subjects actionable rights before the courts against the US authorities.
- The ombudsperson mechanism provided for under the Privacy Shield does not provide a sufficient remedy to make up for this lack of actionable rights, so the Privacy Shield is invalid.
- Regarding transfers under the SCCs, the assessment of the level of protection should consider the protection given by the SCCs and also relevant aspects of the legal system of the destination country when considering access by the public authorities of that third country.
- The SCCs require data exporters and importers to verify, prior to any transfer, whether the level of protection "is respected in the third country concerned." Importers are obliged to notify exporters if they can't comply with the SCCs, and controllers then have an obligation to suspend transfers.
- Data protection authorities should suspend or prohibit transfers of data to a third country if they consider in all the circumstances that the SCCs aren't or can't be complied with in that third country and the protection of the data that is required by EU law cannot be ensured by other means.

On November 11, 2020, the European Data Protection Board (EDPB) published initial guidance on the CJEU's *Schrems II* decision.[2] The guidance was intended to assist controllers and processors in complying with the CJEU's ruling that "data exporters" seeking to rely on the EU's SCCs must (i) conduct a risk assessment of the transfer and, if necessary, (ii) implement "supplementary measures" to protect the data in the recipient country.