Client Alert | Intellectual Property / Technology

EU Data Transfer Restrictions – No changes for now

December 2019

Authors: Tim Hickman, John Timmons

The Court of Justice of the EU ("**CJEU**") is currently hearing a challenge against the validity of two key mechanisms that businesses use to transfer personal data internationally. In a move that will come as a relief to businesses, the Advocate General ("**AG**") of the CJEU has opined that those mechanisms remain lawful.

AG Saugmandsgaard Øe has delivered his opinion in case C-311/18 on the validity of the Standard Contractual Clauses ("**SCCs**") as a data transfer mechanism. The AG also concluded that it was unnecessary for him to opine on the validity of another data transfer mechanism, the EU-US Privacy Shield. If the CJEU follows the AG's opinion, businesses will be able to continue to use SCCs as part of their international personal data transfer strategy, just as they do today. The options available to businesses for international transfers of personal data will remain unchanged.

Although it is not certain that the CJEU will follow the AG's opinion, it is unusual for the CJEU to depart from an AG's opinion without a good reason for doing so. Nevertheless, businesses should consider these issues carefully, to ensure that they are able to react appropriately, in the event that the CJEU reaches a different conclusion.

International transfers of personal data – The requirements

The General Data Protection Regulation ("**GDPR**") restricts the ability of businesses to transfer personal data from within the EEA to any recipient located outside the EEA. The GDPR permits transfers of personal data to non-EEA countries in certain circumstances, including:

- The transfer has been made to a non-EEA country in respect of which the European Commission has issued an Adequacy Decision; the EU-US Privacy Shield Framework is an example of an adequacy decision which permits the transfer of personal data from the EEA to businesses in the United States that are certified under the EU-US Privacy Shield Framework;
- The transfer has been made subject to contractual terms that ensure an adequate level of protection, and that have been approved by the European Commission. Currently, the only approved contractual terms are the SCCs, which permit the transfer of personal data from controllers in the EEA to controllers and/or processors located in non-EEA countries;
- The transfer has been made subject to a code of conduct, or a certification mechanism, approved by the European Commission;
- The transfer has been made on the basis of Binding Corporate Rules ("**BCRs**") that have been approved in accordance with the procedure set out in the GDPR; and
- In the absence of all other safeguards, and in respect of non-recurring transfers of personal data, the transfer has been made subject to one of the derogations set out in Article 49 of the GDPR.

A failure to comply with the GDPR requirements with respect to transfers of personal data to non-EEA countries exposes a business to enforcement action, including the imposition of fines of up to 4% of annual worldwide turnover, or €20million, whichever is greater.

Non-compliance also exposes businesses to the possibility of private litigation in the form of claims being brought by individuals.

The background to the AG's opinion in case C-311/18

In 2015, the validity of the European Commission's Safe Harbour Framework adequacy decision was successfully challenged. The Safe Harbour Framework was established to provide for an efficient and compliant means by which businesses in the EEA could transfer personal data to businesses in the United States. Transfers of personal data were permitted *provided* the relevant business in the United States was self-certified under the Safe Harbour Framework.

The CJEU decided that the Safe Harbour Framework did not provide for adequate protection of personal data, and invalidated the European Commission's adequacy decision (the "**Safe Harbour Decision**"). The Safe Harbour Decision was influenced, in part, by the revelations of former NSA contractor Edward Snowden. The apparent unfettered access that intelligence agencies had to personal data being processed in the United States, including personal data that had been transferred to the United States from the EEA in accordance with the Safe Harbour Framework, was considered fundamentally incompatible with the data protection rights of individuals in the EEA.

In 2016, the EU-US Privacy Shield was introduced, and was specifically designed to address the shortcomings of the Safe Harbour Framework identified by the CJEU.

In the period between the Safe Harbour Decision and the introduction of the EU-US Privacy Shield, many businesses based in the EEA implemented SCCs to ensure that transfers of personal data to the United States remained compliant with data protection laws in Europe.

Memory of the challenges faced by businesses as a result of the Safe Harbour Decision has persisted, and many businesses rely on both the EU-US Privacy Shield, and the SCCs in respect of the same transfers of personal data, to ensure that a contingency plan is in place should the EU-US Privacy Shield be declared invalid in a manner similar to the Safe Harbour Decision.

The AG's opinion

The AG issued his opinion in response to the questions referred to the CJEU by the Irish High Court, which had focused on the validity of the SCCs and the EU-US Privacy Shield. The AG responded to the questions referred by the Irish High Court as follows:

- The provisions of the GDPR relating to transfers of personal data to non-EEA countries are aimed at ensuring the continuity of the high level of protection of personal data once they have been transferred.
- The rationale for the approach adopted in the GDPR is to ensure that the level of protection afforded to personal data processed in Europe is not circumvented by transferring the personal data to a non-EEA country.
- Businesses transferring personal data can rely on adequacy decisions. These decisions represent that the relevant non-EEA country offers a level of protection to personal data (in law and in practice) that is essentially equivalent to the GDPR.
- In the absence of an adequacy decision, businesses can transfer personal data to non-EEA countries subject to the implementation of appropriate safeguards, including by safeguards implemented by contractual means.
- The SCCs provide for an effective transfer mechanism, irrespective of the laws and practices in the non-EEA country to which personal data are transferred. The SCCs "*compensate*" for the deficiencies in protection afforded to personal data in the non-EEA country.

- The fact that the SCCs are not binding on the authorities in non-EEA countries, and therefore do not prevent such authorities from imposing obligations that are contrary to the requirements of the SCCs, does not render the SCCs invalid.
- It must be assessed on a case-by-case basis, by the controller (or relevant data protection supervisory authority) whether the law in the non-EEA country to which personal data are transferred using the SCCs, renders compliance with the obligations in the SCCs impossible. If it does, the transfer should be suspended.

The AG also commented that there is no need for him to opine on the validity of the EU-US Privacy Shield, since this was not directly relevant in the case before the Irish High Court. Nevertheless, the AG did provide a high-level analysis of the validity of the EU-US Privacy Shield Framework, and stated that he "*entertain[s] certain doubts as to the conformity of the 'privacy shield' decision to Article 45(1) of the GDPR*." In light of these comments, businesses that currently rely on the EU-US Privacy Shield Framework, should monitor any future court challenges affecting the EU-US Privacy Shield.

What happens next?

The next step is for the CJEU to consider these questions, and to issue its decision. It is more likely than not that the CJEU will follow the AG's opinion, although it is not obliged to do so. If the CJEU follows the AG's opinion, the practical outcome will be that there will be no material change in the options available to businesses for transferring personal data to non-EEA countries.

Meanwhile, the European Commission is working on updating the SCCs to align more closely with the requirements of the GDPR. Businesses would therefore be well-advised to keep a close eye on developments in this space.

White & Case LLP
5 Old Broad Street
London EC2N 1DW
United Kingdom

T +44 20 7532 1000