EU-US Privacy Shield declared invalid – what's next?

Publication - 22/09/2020

Five years after the Schrems I case[1], which resulted in the Safe Harbour decision[2] being declared invalid, the Court of Justice of the European Union (CJEU) has once again taken a position on two main mechanisms under the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data, and on the free movement of such data (the **GPDR**) with regard to data transfer from the European Union (EU) to the United States of America (US).

On 16 July, the CJEU rendered its long-awaited judgment in the so-called Schrems II case[3], declaring invalid the EU Commission's decision 2016/1250[4] on the adequacy of data protection provided by the EU-US Privacy Shield, one of the foundations for the transfer of personal data to the US. In that same decision, the CJEU confirmed the validity of the EU Commission's decision 2010/87/EC on Standard Contractual Clauses [5] (SCCs), which provides for a legal framework establishing grounds and safeguards for the transfer of personal data to processors located in third countries in the absence of an adequacy decision.

Background of the case

The GDPR lays down specific conditions for transfers of personal data to third countries[6], one of them being the existence of an EU Commission decision on the adequacy of the level of protection the country in question ensures. First such decision related to the US, the Safe Harbour one, was examined in the Schrems I case – the CJEU declared it invalid, as the US legislative framework in the area of data protection neither, inter alia, ensured that access to personal data by national authorities is restricted to what is strictly necessary, nor enabled an individual to pursue legal remedies or demand rectification and deletion of personal data related to themselves.

To ensure transatlantic data flows between the EU and the US following this annulment, the EU Commission and the US government reached a new political agreement on the subject, following which the Privacy Shield decision was adopted in July 2016.

Impact on EU-US Privacy Shield

The CJEU considers that certain limitations on data protection imposed by US law, in particular the possibility for US public authorities to access and use personal data transferred from the EU to the US for national security purposes, do not satisfy the requirements with regard to the principle of proportionality imposed by EU law. The requirements to which such authorities are submitted when implementing surveillance programmes are not equivalent to those required under EU law, as no limitation of their powers is foreseen and no guarantees for potentially targeted non-US persons exist. Further, no actionable rights are being granted to data subjects before a US body.

Impact on Standard Contractual Clauses

The CJEU clarified that the validity of EU Commission decision 2010/87/EC was not called into question by the fact that the standard data protection clauses contained therein were contractual in nature and therefore not legally binding on the authorities of the third country

to which the data was transferred. According to the CJEU, decision 2010/87/EC established effective mechanisms which:

i. ensured a level of protection equivalent to the one guaranteed within the EU by the GDPR, and
ii. provided for a suspension or prohibition of data transfers in case of a breach of obligations under such clauses

In this context, the CJEU highlighted the obligation of both the data exporter and the data importer to verify, prior to any transfer alongside the SCCs and on a case-by-case basis, the level of protection in the third country, and to establish – where necessary - any supplementary measures before proceeding with such transfer. In addition, it is a specific obligation of the data importer to inform the data exporter on any inability to comply with the SCCs, which triggers on the other side the obligation of the data exporter to suspend the relevant transfer and/or terminate the agreement with the data importer. A transfer may also be temporarily or permanently suspended upon the intervention of data protection authorities.

Remaining solutions for data transfers to the US

It is crucial for all concerned persons and entities to assess as soon as possible their current GDPR setup where the transfer of personal data to the US is involved, as there is no grace period safeguarding the effect of the EU-US Privacy Shield.

Nevertheless, it should be recalled that pursuant to the GDPR a transfer of personal data outside of the EU/EEA (including onward transfers) is permissible if the level of protection of natural persons guaranteed by the regulation is not undermined. As one of the potential guarantee mechanisms, the "umbrella" adequacy assessment of the Commission, is no longer eligible, several alternative tools may still be used to ensure a compliant transfer of data prior to further negotiations between the EU and the US on a new set of measures which will comply with the standards set by the CJEU.

It should be noted that data transfer agreements containing SCCs may be put in place. They will not, however, be self-sufficient and an obligation to assess and ascertain the "essential equivalence" of the protection in the third country on a case-by-case basis will have to be satisfied. This may result in the necessity to upgrade the SCCs, and/or establish supplementary measures based on the result of such an assessment. Whether or not the implementation of supplementary measures will be required depends on the result of such assessment in light of the circumstances of the transfer(s). The overarching requirement is to ensure that the SCC, together with any supplementary measures, has the effect of preventing US law from impinging the adequate level of protection. As supplementary measures are of a contractual nature and therefore not binding on US authorities, the effectiveness and adequacy of technical safeguards such as peer-to-peer encryption, tokenisation, access via cloud solutions involving data storage in the EU, or data anonymisation is yet to be assessed and will certainly be addressed in upcoming publications of the EDPB or national authorities.

Binding corporate rules (BCRs) within a corporate group, approved by at least one European data protection supervisory authority, are another viable option. As is the case for SCCs, relying on BCRs will, however, also need to be ascertained by an assessment and flanked – as the case may be – by supplementary measures.

Other possible derogations include approved codes of conduct of associations or bodies representing categories of controllers or processors, approved certification mechanisms, or mechanisms provided under article 49 of the GDPR. These include:

i. consent, which needs to be explicit, specific to a particular transfer or set of transfers, and informed as to the possible risks;

i. transfers which are objectively necessary for the conclusion or performance of a contract or the exercise of legal claims;

i. transfers necessary for important reasons of public interest on a small scale and not in a systematic manner and;

i. occasional and limited transfers necessary for compelling legitimate interests of the controller which are not overridden by the interests or rights and freedoms of the data subject.

The EDPB has emphasised that relying on derogations under article 49 should not become a rule in practice and that data exporters need to ensure that the transfer is restricted to specific situations and that it meets the strict necessity test.

In light of the new CJEU decision, the European Data Protection Board (EDPB) announced that it will clarify and provide guidance on the kind of supplementary measures that could be established in addition to SCCs/BCRs, whether of legal, technical or organisational nature, in case the transfer of data to third countries is not yet sufficiently protected by SCCs or BCRs. EDPB also stressed that the national competent authorities " will also have a key role to play when enforcing the GDPR and when issuing further decisions on transfers to third countries". Some national data protection authorities, including the Luxembourg Commission Nationale pour la Protection des Données (CNPD), have issued statements on the subject. The CNPD has noted that it is currently assessing the impact to ensure consistency across the EEA, working closely with its counterparts to ensure that further guidance is provided to organisations and businesses.

To find out more on how to assess your current and future data transfers to the US, please contact one of our team members.

---

[1] C-362/14 - Maximillian Schrems v Data Protection Commissioner.

[2] Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the Safe Harbour privacy principles and related frequently asked questions issued by the US Department of Commerce – previous Commission adequacy decision, which was annulled in the above case due to the absence of sufficient guarantees that the data transferred will be protected from US government intervention.

[3] C-311/18 - Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems.

[4] Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield.

[5] Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46 (OJ2010 L39, p.5), as amended by Commission Implementing Decision (EU) 2016/2297 of 16

December 2016.

[6] Articles 44 to 50

About Ogier

Ogier provides practical advice on BVI, Cayman Islands, Guernsey, Jersey and Luxembourg law through its global network of offices. Ours is the only firm to advise on these five laws. We regularly win awards for the quality of our client service, our work and our people.

Disclaimer

ogier.com

Key Contacts

Benot Rose
Partner
Luxembourg Legal
benoit.rose@ogier.com
T+352 2712 2065
M+352 691 302 065

Milan Hauber
Senior Associate
Luxembourg Legal
milan.hauber@ogier.com
T+352 2712 2067
M+352 691 442 067

Related services

GDPR