The CJEU judgment in the *Schrems II* case

In its July 2020 *Schrems II* judgment, the Court of Justice of the European Union (CJEU) declared the European Commission's Privacy Shield Decision invalid on account of invasive US surveillance programmes, thereby making transfers of personal data on the basis of the Privacy Shield Decision illegal. Furthermore, the Court stipulated stricter requirements for the transfer of personal data based on standard contract clauses (SCCs). Data controllers or processors that intend to transfer data based on SCCs must ensure that the data subject is granted a level of protection essentially equivalent to that guaranteed by the General Data Protection Regulation (GDPR) and the EU Charter of Fundamental Rights (CFR) – if necessary with additional measures to compensate for lacunae in protection of third-country legal systems. Failing that, operators must suspend the transfer of personal data outside the EU.

Background

The Privacy Shield framework provides for the possibility of lawful transfer of personal data from the EU to the United States (US), while ensuring a strong set of data protection requirements and safeguards. On the basis of this framework EU (and later European Economic Area, EEA) businesses were able to legally transfer personal data to US-based companies that were listed in the Privacy Shield list. Admission to this list is administered by the US Department of Commerce, while the US Federal Trade Commission monitors compliance. While participation is voluntary, companies that have been certified are obliged to comply with the Privacy Shield Principles, as they became enforceable under US law. A case of unjustified non-compliance could trigger a case pursuant to section 5 of the Free Trade Commission Act, or lead to the organisation's removal from the Privacy Shield list.

The July 2020 ruling is in line with the Court's persistent strengthening of the level of protection in recent years. Notably, the CJEU annulled in 2006 the 2004 Passenger Name Record (PNR) Agreement between the EU and the US, objected to the entry into force of the EU-Canada PNR Agreement in its Opinion 1/15 issued in 2017 and invalidated the Safe Harbour Decision in the *Schrems I* judgment in 2015. The Privacy Shield principles became operational as a replacement for the invalidated Safe Harbour principles on 1 August 2016. Although it addressed many of the defects of its predecessor, its remaining privacy lacunae were repeatedly criticised, in particular in a 2018 resolution of the European Parliament and by the European Data Protection Board (EDPB). In February 2020, the Chair of the Parliament's Civil Liberties Committee also expressed his concerns after a delegation visit to the United States. The European Commission, by contrast, reaffirmed the mechanism by holding that the US level of data protection was adequate in its 2019 third annual review of the Privacy Shield.

Judgment

Following the *Schrems I* judgment, Facebook Ireland explained that it transferred much of the data to its US parent company based on SCCs. On 1 December 2015, Max Schrems reformulated his complaint lodged with the Irish Data Protection Authority (DPA) to the effect that the SCC Decision was not able to justify the transfer of personal data to the US, since US surveillance programmes interfered with his fundamental rights to privacy, to data protection and to effective judicial protection. In a draft decision, the DPA shared Schrems' concerns and brought an action before the Irish High Court, which then made reference to the Court for a preliminary hearing. In the meantime another transfer mechanism, the Privacy Shield Decision, became pertinent to the case, which prompted the CJEU also to rule on the validity of this instrument.

On 16 July 2020, the CJEU (i) declared invalid the European Commission's Privacy Shield Decision and (ii) affirmed the validity of the SCC Decision while stipulating stricter requirements for SCC-based transfers.

(i) The Court held that the US does not provide for an *essentially equivalent*, and therefore sufficient, level of protection as guaranteed by the GDPR and the CFR. The legal bases of US surveillance programmes such as PRISM and UPSTREAM are not limited to what is strictly necessary and would be considered a disproportionate interference with the rights to protection of data and privacy (Article 45(1) GDPR, read in

Author: Hendrik Mildebrath, Members' Research Service
PE 652.073 – September 2020

light of Articles 7, 8 and 52(1) CFR), since they do not sufficiently limit the powers conferred upon US authorities and lack actionable rights for EU subjects against US authorities. Contrary to the European Commission's adequacy findings, the Ombudsman mechanism does not remedy, but rather exacerbates these deficiencies, as the mechanism interferes with the right to effective judicial protection (Article 45(1) GDPR, read in light of Article 47 CFR), due to concerns over the independence of the institution and on the enforceability of its decisions.

(ii) Additionally, the Court affirmed the validity of the SCC Decision and held that SCCs do not, per se, present lawful or unlawful grounds for data transfer (no panacea). The CJEU also stipulates that data controllers or operators that seek to transfer data based on SCCs, must ensure that the data subject is afforded a level of protection *essentially equivalent* to that guaranteed by the GDPR and CFR – if necessary with *additional measures* to compensate for lacunae in the protection of third-country legal systems. Failing that, operators must suspend the data transfer. Supervisory authorities must check transfers and are *required* to prohibit transfers where they find that data subjects are not afforded essentially equivalent protection.

Implications and first reactions

Implications for commercial data transfers

As a result of the Court's decision, EU companies can no longer legally transfer data to the US based on the Privacy Shield framework. Companies that continue to transfer data on the basis of an invalid mechanism risk a penalty of €20 million or 4 % of their global turnover, pursuant to Article 83(5)(c) GDPR.

However, commentators disagree on the broader implications of the Court ruling for operators. Some commentators believe that the vast majority of companies can continue using the conventional SCCs, while others argue that companies should – if at all – only use SCCs for transfers to the US, if (i) they are not subject to the respective surveillance law, or if (ii) they provide for 'additional safeguards'. The DPA of North Rhine-Westphalia pointed out that any companies using US communication services or transatlantic cables might be subject to US surveillance mechanisms. To salvage SCC-based data transfers, such companies would need to compensate for gaps in protection with – so far undetermined – 'additional safeguards'. The Court stressed that protective contract clauses are not binding on third parties or authorities and therefore likely to be ineffective, while cryptanalytic and quantum computing efforts of intelligence agencies raise concerns about the effectiveness of protective technical measures such as encryption.

According to the EDPB and the Conference of the German Data Protection Authorities (DSK), companies may transfer data based on binding corporate rules, but will have to, equally, ensure the essential equivalence. Although the EDPB affirms the possibility of transferring data on the basis of derogations provided in Article 49(1)(a) GDPR, its guidelines raise doubts on their suitability to legitimise recurrent transfers. Furthermore, the EDPB announced that it will not suspend enforcement for a regulatory grace period. The Berlin, Hamburg and Dutch DPAs advise halting transfers to the US. The Berlin DPA even advises to retrieve data from the US. Many DPAs stress the need for further analysis and case-by-case assessments.

Implications for international relations

US Secretary of Commerce Wilbur Ross and US Secretary of State Mike Pompeo expressed their deep disappointment with the ruling and suggested possible adverse effects on the US$7.1 million transatlantic economic relationship. Both stressed the importance of data flows for economic growth as well as for the post-Covid-19 recovery and pledged to work closely with the EU. European Commission Vice-President Věra Jourová and Commissioner Didier Reynders committed to joint efforts, and suggested modernising standard contract clauses. While DigitalEurope and others would welcome a third longer-lasting adequacy agreement, BusinessEurope advocates an additional intermediate solution to avoid a negative impact on the economy. Max Schrems and the European Data Protection Supervisor encourage the United States to reform surveillance laws and meet the requirements of the Court. However, it is reported that senior US officials do not consider such an overhaul 'advisable' or 'possible' in the short term. The rationale of this ruling will particularly impact those third countries which conduct extensive surveillance for national security. This might become relevant for the United Kingdom, as it will be treated as a third country post-Brexit. Some commentators suggest that this ruling promotes a world fractured into data spheres of influence. Conversely, the judgment might bolster the European Commission's objective to 'promote convergence of data protection standards at international level, as a way to facilitate data flows and thus trade'.