CJEU judgment on cross-border data transfers from the EU to third countries – what now?

Daniela Fábián Masoch, Lucas Maciejewski

3 August 2020

On 16 July 2020, the Court of Justice of the European Union (CJEU) delivered its judgment in Case C-311/18 — *Data Protection Commissioner v. Facebook Ireland and Maximillian Schrems* (so-called "Schrems II"). In this case, M. Schrems requested the Commission to prohibit or suspend the transfer by Facebook Ireland of his personal data to Facebook Inc., established in the US, on the ground that that third country did not ensure an adequate level of protection. This ruling has far-reaching consequences for any transfers of data from the EU to third countries.

The CJEU's findings of the decision

1. Privacy Shield

The CJEU invalidated, with immediate effect, the European Commission Decision 2016/1250 on the transfer of personal data to the US (Privacy Shield). The rationale for this decision is in essence that US law as evaluated by the CJEU, in particular Section 702 Foreign Intelligence Surveillance Act "FISA" and Executive Order 12333, does not provide a level of protection substantially equivalent to that in the EU (in terms of appropriate safeguards, enforceable rights and effective legal remedies required by the GDPR).

Please note that the Swiss Data Protection Authority (FDPIC) has taken note of the CJEU ruling. This ruling is not directly applicable to Switzerland and, therefore, to the CH-US Privacy Shield. The FDPIC will examine the judgment in detail and comment on it in due course. While the CH-US Privacy Shield is, at the moment, still valid, it is to be expected that the authority will follow the CJEU ruling and invalidate the CH-US Privacy Shield as well (as it did in 2015 after the invalidation of the Safe Harbor arrangement).

2. Standard Contractual Clauses (SCC)

The CJEU confirmed the validity, in principle, of the Commission Decision 2010/87/EC on Standard Contractual Clauses (SCC). However, the CJEU stressed the responsibility of the data exporter and data importer to carry out a case-by-case analysis of the domestic law of the data importer, specifically concerning access by public authorities and judicial redress to determine whether the rights of data subjects in the third country enjoy a level of protection equivalent to that in the Union. Where this is not the case, data exporters must take additional, effective safeguards or suspend the data transfer in question. Such additional safeguards may include technical measures such as encryption of the data in transit and at rest, contractual safeguards, or organizational measures. The CJEU does not, however, specify what kind of additional safeguards should be taken and thus leaves companies in uncertainty. More guidance is expected in the near future.

The obligations highlighted by the CJEU are not new. They are already included both in the Controller to Processor SCC and in the Controller to Controller SCC. The CJEU calls upon the existing obligations of companies which export, and import, personal data based on SCC from the EU to a third country without adequacy finding by the EU Commission, and stresses

that it is not enough to sign the SCC, but that the parties must examine on a case-by-case basis whether the SCC can be complied with in the recipient country.

The CJEU decision concerns, in principle, the Controller to Processor SCC. However, the same arguments apply to any transfer of personal data from the EU to a third country, including on the basis of Controller to Controller SCC or Binding Corporate Rules (BCR).

Companies that do not carry out this analysis and possibly transfer personal data based on SCC to a third country, where the data recipient is not able to effectively comply with SCC due to conflicting local legislation, violate the requirements under the GDPR (even if SCC have been signed) and therefore risk hefty fines of up to EUR 20'000'000 or 4% of the annual turnover of the preceding year, whichever is higher. Also, such transfers may be prohibited or suspended by the competent supervisory authorities.

Relevant clauses in the current SCC

Controller to Processor SCC of 5 February 2010 (2010/87/EU)

Clause 4 (a): The data exporter agrees and warrants that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (…) and does not violate the relevant provisions of that State.

Clause 5: The data importer agrees and warrants:

(a): to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract.

(b): that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract.

Controller to Controller SCC of 27 December 2004 (2004/915/EC)

Clause I (b): The data exporter warrants and undertakes that it has used reasonable efforts to determine that the data importer is able to satisfy its legal obligations under these clauses.

Clause II (c): The data importer warrants and undertakes that it has no reason to believe, at the time of entering into these clauses, in the existence of any local laws that would have a substantial adverse effect on the guarantees provided for under these clauses, and it will inform the data exporter (which will pass such notification on to the authority where required) if it becomes aware of any such laws.

Reactions of data protection authorities

In the meantime, several data protection authorities as well as the European Data Protection Supervisor (statement 17 July 2020), the European Data Protection Board (statement 17 July 2020) and the German Conference of the Independent Data Protection Authorities of the Federal Government and the Länder (Datenschutzkonferenz - DSK) (press release 28 July 2020) have issued initial guidance for how to handle data transfers in future. You may find the respective references to the guidance on the IAPP Resource Center page.

Some data protection authorities, such as the German data protection authorities in Berlin (press release 17 July 2020) and Hamburg (press release 16 July 2020) have issued rigorous statements on the unlawfulness of data transfer to the US, based on SCC. The Berlin data protection authority is even calling on all those responsible under its supervision not to transfer personal data to the USA any longer, but to switch immediately to service providers based in the EU or another third country with an adequate level of protection.

The EDPB has issued, in addition to its statement, FAQ. More guidance, in particular regarding the additional safeguards to be taken, is expected.

What companies can do

While it is expected that the EDPB, the EU Commission and the supervisory authorities provide further guidance on the "additional safeguards"; and the EU Commission issues revised SCC, data exporters and importers should consider additional safeguards to ensure an adequate level of protection when transferring personal data from the EU to third countries:

1. Continue to monitor guidance issued by the EDPB, the EU Commission, and various supervisory authorities and the issuance of revised sets of SCC;
2. Identify and document any cross-border data transfer within your organization and to vendors and other business partners located outside of the EU/CH:
    a. If any personal data is transferred cross-border based on EU-US Privacy Shield, determine alternative legal mechanisms to enable such transfers under the GDPR (such as SCC subject to the conditions outlined by the CJEU, or one of the legal derogations under art. 49 GDPR), and amend contracts accordingly. Create a plan outlining all steps, responsibilities and timelines, including the possible termination of the EU-US Privacy Shield in accordance with the notification requirements, and adhere to the plan.
    b. If any personal data is transferred cross-border based on SCC (including intragroup data transfer agreements), assess, together with the data importer, whether the legislation of the third country of destination ensures adequate protection under EU law of personal data transferred under the SCC. In particular, it should be assessed if the data importer is subject to any law and practice that allows data access by public authorities (such as under Art. 702 FISA in the US), and therefore the data importer may not be able to comply with the SCC. In this case, the data exporter shall conduct a privacy risk assessment to evaluate the likelihood of disclosure or access, the sensitivity and the volume of the data, and the retention period, and consider additional safeguards beyond SCC, including, for example, contractual and technical measures such as data encryption in transit and at rest. If such other measures are not possible, the data exporter should suspend or end the transfer of personal data, or notify the competent supervisory authority, which may ban any further data transfer.
    c. If the transfer is based on BCR, the same analysis as for SCC should be conducted.
    d. If the transfer is based on one of the legal derogations provided by Art. 49 GDPR, such as explicit consent or the necessity to perform a contract, no further steps are required for now.
3. Document the analysis, the outcome, and any steps taken.
4. Review and amend due diligence processes and contractual templates:
    a. To be able to conduct appropriate conformity and risk assessments, the due diligence process and the questionnaire for data protection assessments of vendors should be revised to include questions about the existence of monitoring and data access laws and practices to which the data importer is subject. Particular attention should also be paid to the data importer's internal rules and procedures concerning the handling of requests from public authorities and notification to the data exporter. Also, any data importers, i.e., processors and controllers, should be evaluated in the future.
    b. The contractual language in templates regarding the cross-border data transfers should be revised to emphasize the primary obligations of the data exporter/importer arising from the SCC itself, the handling of government requests to access personal data, and removing any reference to the Privacy Shield Framework.
5. Service providers (data importers) may assist their customers by conducting a thorough analysis to verify the adequacy of EU laws and comply with the SCC (such exercise may also help to maintain a competitive edge).
6. Establish (or revise) internal policies and procedures to address cross-border requirements in compliance with the GDPR and the CJEU judgment.
7. In the long-term, companies may consider moving to more robust data transfer mechanisms, as provided in Art. 46 GDPR, such as binding corporate rules (BCR for Controllers and BCR for Processors) which are approved by the EU supervisory authorities, code of conduct, or certification mechanisms.