The Computer & Internet Lawyer

Volume 37 ▲ Number 9 ▲ October 2020

Ronald L. Johnston, Arnold & Porter, LLP, Editor-in-Chief

Schrems II: History Repeats Itself, But It Is Not All Bad News for International Data Transfers

By Cynthia O'Donoghue, Philip Thomas, Sarah O'Brien, Andreas Splittgerber, Christian Leuthner, and Elle Todd

The Court of Justice of the European Union ("CJEU") has handed down its judgment on a case brought by privacy rights activist Max Schrems ("Schrems II").[1] The case concerned the transfer of personal data to recipients in the United States via the EU Commission standard contractual clauses ("SCCs") and questioned the validity of the EU–U.S. Privacy Shield ("Privacy Shield"). The ruling affects not just transfers of personal data from the EU to the United States but also applies to all transfers of personal data from the EU to countries outside the EEA.

In summary, the CJEU has:

- Invalidated the use of the Privacy Shield as an adequate safeguard when transferring personal data outside the EEA to the United States – primarily due to potential unrestricted U.S. government access.

- Found the SCCs to be an adequate safeguard when transferring personal data outside the EEA to third parties. However, depending on the prevailing position in a particular third country, the adoption of supplementary contractual provisions by the controller to ensure compliance with that level of protection afforded in the SCCs may be required.

To conclude, all data transfers from the EEA to countries outside the EEA will have to be assessed on a case-by-case basis to determine whether additional clauses, in addition to those afforded under the SCCs or even under binding corporate rules, have to be implemented by organizations. It is expected that EU data protection authorities will grant more guidance regarding specific countries.

Cynthia O'Donoghue, a partner in the London office of Reed Smith LLP, is the Deputy Practice Group Leader of the firm's IP, Tech & Data Group. **Philip Thomas**, a partner in the firm's London office, is a member of the firm's Information Technology, Privacy & Data Security team and of its IP, Tech & Data Group. **Sarah O'Brien**, an associate in the firm's London office, in its IP, Tech & Data Group. **Dr. Andreas Splittgerber** is a partner in the firm's Munich office and a member of its IP, Tech & Data Group. **Christian Leuthner** is an associate in the firm's Frankfurt office and a member of its IP, Tech & Data Group. **Elle Todd**, a partner in the firm's London office, practices digital and data law. The authors may be contacted at codonoghue@reedsmith.com, pthomas@reedsmith.com, sobrien@reedsmith.com, asplittgerber@reedsmith.com, cleuthner@reedsmith.com, and etodd@reedsmith.com, respectively.

Background

The background to this case is a complex one. The case is the continuation of an earlier complaint made by Schrems against Facebook in 2013. In 2013, Schrems filed a complaint with the Irish data protection authority claiming that Facebook's transfer of EU citizens' personal data under the Safe Harbor framework to Facebook in the United States violated their rights.

In a landmark finding in October 2015,[2] the CJEU held that the Safe Harbor framework was invalid ("Schrems I"). Among other reasons, this decision was based on the fact that U.S. legislation did not limit the interference with an individual's rights to what is strictly necessary.

Since then, Schrems reformulated his complaint and decided to challenge the transfers of personal data to the United States performed on the basis of SCCs.[3] The use of SCCs was the alternative mechanism Facebook relied on to legitimize EU to U.S. data flows, as they could no longer rely on the Safe Harbor provisions following Schrems I.

Following its investigation into Schrems' reformulated complaint, the Irish data protection authority published a draft decision where it took the view that personal data transferred to the United States was likely to be consulted and processed by certain U.S. authorities in a manner incompatible with Articles 7 and 8 of the Charter of Fundamental Rights of the European Union ("Charter").[4] The Irish data protection authority further concluded that U.S. law did not provide EU citizens with the equivalent to an effective judicial remedy in accordance with Article 47 of the Charter, and that the SCCs were not capable of remedying this defect.

The Irish data protection authority brought the Schrems II proceedings before the Irish High Court who referred 11 questions for a preliminary ruling (*see* below). In an annex to the referral, the Irish High Court included a copy of a judgment it handed down on October 2017 in which it had set out the results of an analysis of the evidence before it in a national proceeding in which the U.S. government had participated. In this judgment, the Irish High Court agreed with the Irish data protection authority regarding the lack of effective judicial remedies and further concluded that the appointment of a Privacy Shield ombudsperson did not remedy this defect.

The key questions referred to the CJEU included:

- Whether transfers of personal data to the United States pursuant to the SCCs breach Article 7 (privacy) and Article 8 (data protection) rights under the Charter.

- Whether the use of SCCs for transfers of personal data to third countries offers sufficient safeguards as regards to the protection of those freedoms and fundamental rights.

- Whether the laws and practices in third countries are relevant when considering whether SCCs can be relied on to legitimize transfers of personal data to third countries.

- Whether, if a third country data importer under the SCCs is subject to surveillance laws that, in a data protection authorities view, conflict with the SCCs and/or the Charter, the data protection authority is required to suspend data flows or whether it can use its discretion not to suspend data flows. If the former, the question is whether the power to suspend is limited.

- Whether the Privacy Shield constitutes a finding of adequacy, binding on all data protection authorities and the courts of member states.

- What role, if any, the European Commission's adequacy decision relating to the Privacy Shield has on evaluating the transfers of personal data to the United States based on SCCs.

The Irish High Court will, as a next step, have to apply the CJEU decision to the Schrems II case.

Legal Framework

The General Data Protection Regulation ("GDPR") (and its predecessor, the Data Protection Directive) provides that personal data may be transferred to a third country if that country ensures an adequate level of data protection. SCCs and the Privacy Shield were two of several mechanisms approved by the European Commission for personal data transfers to countries not found to offer adequate protection for personal data and to the United States, respectively.

AG Opinion

As is common practice with all CJEU cases, an advocate general ("AG") publishes an opinion on a case prior to the CJEU's judgment. In this case, AG Henrik Saugmandsgaard Øe published his opinion on December 19, 2019.

In summary, the key findings of the AG were as follows:

- The SCCs are valid.
- The main purpose of the SCCs is to compensate for any deficiencies in the protection afforded by the third country of destination, which the data exporter and importer contractually undertake to respect.
- He did not make a finding in relation to the adequacy of the Privacy Shield.

CJEU's Judgment

The key findings of the CJEU are as follows:

- In practice, the SCCs, the implementing European Commission decision and/or various provisions of the GDPR provide for an effective mechanism for EU-based controllers and national supervisory authorities to suspend or prohibit the transfer of personal data to third countries that do not offer adequate protection for data subjects' rights. The CJEU, therefore, sees no reason to invalidate the use of SCCs as a valid transfer mechanism.
- The legal systems of third countries is relevant when assessing whether SCCs can be relied on to legitimize transfers of personal data to third countries. Specifically, the aspects set out in Article 45(2) of the GDPR[5] must be taken into account when making this assessment. These aspects include the rule of law, respect for human rights and fundamental freedoms, relevant legislation and the implementation of such legislation, the existence and effective functioning of one or more independent data protection authorities and the international commitments the third country concerned has entered into, in particular, in relation to the protection of personal data.
- Unless the European Commission has issued an adequacy decision in relation to a particular third country, a national data protection authority is required to suspend or prohibit personal data transfers under SCCs where:
    - That national supervisory authority believes the SCCs are not or cannot be complied within the third country.
    - The protection of the personal data transferred cannot be ensured by other means.
- The CJEU has found it impossible to conclude that U.S. law ensures a level of protection essentially equivalent to that guaranteed under EU law. Specifically, the CJEU determined that:
    - U.S. surveillance laws relating to the accessing and use by U.S. public authorities of personal data transferred from the EU go beyond what is strictly necessary to safeguard its national security.
    - Notwithstanding the appointment of a Privacy Shield ombudsman (whose decisions do not bind U.S. intelligence services), EU data subjects have no right under U.S. law to an effective remedy for breach of their fundamental rights and freedoms.

Impact for Organizations

SCCs

Organizations relying on SCCs to legitimize their transfers of personal data to third countries (the United States and all other non-EEA countries) can take (some) comfort from this judgment. The judgment, however, also shines a very bright light on the obligations set out in the SCCs and reminds controllers that they are under an obligation to verify, on a case-by-case basis, whether the law in the third country of the recipient ensures adequate protection for data subjects' fundamental rights and freedoms under EU law. Where the controller exporting data, or the data importer, determine that such a third country does not provide adequate protection, even with additional contractual provisions to those offered under the SCCs, the SCCs provide for a number of consequences, including suspension of the transfer, return of the data and possibly even informing the data subjects.

The CJEU suggests the following in paragraph 132 of the decision: "In that regard, recital 109 of the regulation states that *'the possibility for the controller . . . to use standard data-protection clauses adopted by the Commission . . . should [not] prevent [it] . . . from adding other clauses or additional safeguards'* and states, in particular, that the controller *'should be encouraged to provide additional safeguards . . . that supplement standard [data] protection clauses.*'" In theory, this sounds positive, but the key will be finding a practical way to implement it.

Privacy Shield

Organizations that rely on the Privacy Shield (and/or the Swiss–U.S. Privacy Shield, as the Swiss authorities are likely to follow the CJEU in invalidating this mechanism) will need to work quickly to legitimize their

personal data transfers to the United States by adopting an alternative mechanism. It is unclear at the time of writing whether data protection authorities will offer a grace period to allow organizations to do this.

All Data Transfers Outside the EEA Are Affected

The judgment also has wider implications than just transfers of personal data from the EEA to the United States, as it will also affect those countries outside the EU that recognize the Privacy Shield as an adequate safeguard for transfers of personal data from their territory to the United States. These countries include the United Kingdom (post the transition period), Israel, and Serbia, among others.

For Organizations Involved in Data Transfers from the EEA to Non-EEA Countries

The implications of the judgment for organizations are several fold. Not only does it affect any transfers of data from the EU within their organization, it affects all transfers of data within a supply chain, such that organizations will need to assess transfers of data to vendors that have certified to the Privacy Shield as well as to vendors that transfer data based on the use of SCCs.

There are a number of steps that organizations will need to take, such as assessing the adequacy of their data transfer mechanisms, legal bases for transfers, availability of exemptions, availability of alternative transfer mechanisms and safeguards for data transfers in relation to access by governmental authorities under the laws of the place of transfer, or even under laws where there is long-arm or extraterritorial jurisdiction, as can be the case with affiliates of U.S. parent companies.

Notes

1. C-311/18, *Data Protection Commissioner v. Facebook Ireland Limited, Maximillian Schrems*, *available at http://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=9798635*. The CJEU's press release is *available at https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091en.pdf*.
2. *http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=83563&cm_mid=5053745&cm_crmid=abe5fd09-ad2e-de11-b65e-0013211fcd8f&cm_medium=email*.
3. *https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32010D0087*.
4. *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A12012P%2FTXT*.
5. *https://eur-lex.europa.eu/eli/reg/2016/679/oj*.