A new approach on international data transfers is required

SUMMARY

CONTACTS

Cláudia Fernandes Martins
cmartins@macedovitorino.com

André Feiteiro
afeiteiro@macedovitorino.com

Overview

On January 15, 2021, the European Data Protection Board (EDPB) and European Data Protection Supervisor (EDPS) adopted a joint opinion on the draft proposal of Standard Contractual Clauses (SCCs) released by the European Commission on November 12 2020 for data transfers from within the EEA to non-EEA countries (third countries) (the Draft SCCs).

Once settled, the Draft SCCs will replace the existing SSCs: (i) EU controller to non-EU or EEA controller (Decision 2001/497/EC and Decision 2004/915/EC) and EU controller to non-EU or EEA processor (Decision 2010/87/EU), approved under the former Data Protection Directive and that was repealed by the EU General Data Protection Regulation (GDPR).

GDPR requires a solution to be implemented for data transfers from the European Economic Area (EEA) to third countries that do not provide an adequate level of data protection. The SCCs, among or together with other options, such as data subject's consent, binding corporate rules (BCR), ad hoc contractual clauses, approved codes of conduct or certification mechanisms, allow international data transfers in compliance with GDPR.

The EU-US Privacy Shield was also one of the solutions used to justify data transfers from EEA to the US. Last summer, the EU-US Privacy Shield was, however, ruled void by the Court of Justice of the European Union's (CJEU), in Schrems II case. Consequently, organizations using the EU-US Privacy Shield need to rely on alternative solutions, from which SCCs may be used to justify data transfers to the US.

For a comprehensive approach, we will first recall the Schrems II case and the subsequent steps until the recent joint opinion issued by EDPB and EDPS.

Schrems II case

This decision of July 16 2020 (Schrems II case) is the sequel to a previous ruling, where CJEU invalidated the EU-US Safe Harbour (Schrems I case). The EU-US Safe Harbour was the predecessor of the Privacy Shield, which also ruled as inadequate to ensure an adequate level of protection required for international data transfers. In turn, CJEU considered the Commission Decision 2010/87/EU applicable to data transfers from EU controllers to non-EU or EEA processors to be valid.

This CJEU ruling follows a complaint lodged by M. Schrems. The Austrian citizen and Facebook's user lodged his complaint with the Irish data supervisory authority seeking to prohibit Facebook Ireland from transferring his personal data to the US. Personal data of Facebook users, who are residents in the EU, is transferred to servers of Facebook Inc. located in the US where they are processed under International SCCs.

«The technologies of the Fourth Industrial Revolution, including artificial intelligence (AI), the internet of things (IoT) and blockchain, are exceptionally reliant on accessing and processing data. To realize the potential of such data-intensive technologies, or to fully harness the power and efficiency of cloud computing solutions for start-ups and SMEs, data needs to be able to move seamlessly across country borders.»

World Economic Forum, A Roadmap for Cross Border Data Flows: Future-Proofing Readiness and Cooperation in the New Data Economy, 9 June 2020

IDC's "Data Age 2025" whitepaper foresees that, «in 2025, 175 zettabytes (175 trillion gigabytes) of new data will be created around the world.»

M. Schrems claimed that International SCCs would not offer sufficient protection against access by US public authorities to the data transferred to the US.

Following the Advocate General's Opinion (non-binding opinion published on 19 December 2019) on this case, the CJEU considered International SCCs as adequate. The Court points out that International SCCs decision imposes an obligation on the data exporter and on the data recipient to verify, prior to any transfer, whether that level of protection is respected in the receiving country and that the decision requires the recipient to inform the data exporter of any inability to comply with International SCCs, the latter then being, in turn, obliged to suspend the transfer of data and/or to terminate the contract with the former.

On the other hand, CJEU challenged the level of protection afforded by the Privacy Shield on the grounds that it does not include satisfactory limitations to ensure the protection of EU personal data from access and use by US public authorities based on US domestic law.

The Schrems II case has relevant implications on the data transfer from the EU to third countries (namely the US) and gave data subjects, controllers, and processors with a great deal of uncertainty in relation to the conditions under which data exports can occur, i.e. what the practical consequences for existing and new contracts are and how to conduct Transfer Impact Assessments (TIAs) onwards.

SCCs meet businesses halfway

Further to the Schrems II ruling, on 10 November 2020, the EDPB adopted recommendations on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data.

The EDPB recommendations emphasizes the principle of accountability under which controllers which export personal data must ensure that whatever mechanism and supplemental measures govern a data transfer, the data must receive the same protection it would in the EU. Otherwise, the data transfer will breach GDPR. These recommendations are targeted to both public and private transfers of EU data to private sector entities outside the EU.

Data exporters need to determine whether they must use supplemental measures other than the revised SCCs. EDPB provides examples of supplementary measures to be assessed on a case-by-case basis, such as "flawlessly implemented" encryption and pseudonymizing data.

Two days after the EDPB's recommendations, the Commission published the Draft SCCs with input due by December 10, 2020. As data processing is increasingly complex, the adage of this draft proposal is adaptability.

The Draft SCCs combine general clauses with a modular approach to cater for various transfer scenarios. In addition to the general clauses, controllers and processors should select the module applicable to their situation among the four following modules: (i) module one: transfer controller to controller; (ii) module two: transfer controller to processor; (iii) module three: transfer processor to processor; and (iv) module four: transfer processor to controller.

Some relevant issues that should be concerning to organizations dealing with international data transfers, and that do not solve any of the issues raised by the Draft SCCs, include:

- On the adequacy of the law and practices of the third country. This is not a great relief for controllers and processors who come about a great deal of responsibility;
- A brief period of one year to comply. Organizations will need to put in practice the revised SCCs for their entire business operation. The draft proposal grants organizations one year to do so, which may come up short;
- The revised SCCs are not necessarily of use, or mandatory, for organizations operating under SCCs of greater privacy assurance. SCCs work as a minimum protection threshold.

Failure to comply with international data transfer rules may be fined up to €20 million or 4% of the total worldwide annual turnover, plus reputational risk of compliance failures.

Joint opinion of EDPB and EDPS

In this context, on November 12 2020, the Commission requested EDPB and EDPS to issue a Joint Opinion on the Draft Decision and the Draft SCCs ("the Joint Opinion").

In general, EDPB and EDPS are of the opinion that the Draft SCCs offer a reinforced level of protection for data subjects. In particular, EDPB and EDPS welcome the specific provisions intended to address some of the main issues identified in the Schrems II ruling.

Nevertheless, EDPB and EDPS are of the understanding that several provisions could be improved or clarified, including (i) the scope of SCCs; (ii) certain third-party beneficiary rights; (iii) certain obligations regarding onward transfers; (iv) aspects of the assessment of third country laws regarding access to public data by public authorities; and (v) the notification to the supervisory authority.

The conditions under which SCCs can be used must be clear for organizations and data subjects should be provided with effective rights and remedies. SCCs should include a clear distribution of roles and of the liability regime between the parties. Regarding the need, in certain cases, for ad-hoc supplementary measures to ensure that data subjects are afforded a level of protection essentially equivalent to that guaranteed within the EU, the Joint Opinion considers that new SCCs will have to be used along with EDPB Recommendations on supplementary measures.

EDPB and EDPS thus invite the Commission to refer to the final version of EDPB Recommendations on supplementary measures.

The revised SCCs together with the recent Schrems II will give a new approach to international data transfers, with due diligence measures towards data exporters to ascertain whether the country of the data importer effectively ensures an adequate level of protection. For data exporters, this may however become a huge task, as they will need to map all transfers and understand the laws and practices of the third country to adopt appropriate measures to meet the EU's data protection requirements.