Data Privacy and Cybersecurity

EDPB Provides Guidance on Personal Data Transfers Following *Schrems II*

By: Kelly Hagedorn, David P. Saunders, and Matthew Worby

Earlier this year, in *Schrems II*, the Court of Justice of the EU (CJEU) invalidated the EU-US Privacy Shield.[1] That judgment also cast doubt over the validity of standard contractual clauses (SCCs) as a means by which to transfer personal data outside of the EU, in particular to the United States. Unsurprisingly, this has caused concern within organisations who rely on such transfers as part of their business model.

Data protection requirements, imposed by the GDPR, travel with any personal data whenever it is transmitted outside of the EU. Problems arise when an organisation needs to transfer personal data to a jurisdiction where local laws might undermine these protections. Without some way to manage this potential conflict, it was unclear if organisations' personal data transfers outside of the EU would be able to continue.

Unfortunately, the CJEU provided no practical guidance for organisations as to how to make international personal data transfers compliant with its ruling and did not provide any safe harbour period before its ruling took effect. In recent days, however, two key efforts have been made to assist organisations meet their post-*Schrems II* GDPR requirements:

1. recommendations have been issued by the European Data Protection Board (EDPB);[2] and
2. a revised set of SCCs has been published by the European Commission for consultation.

Recommendations Issued by the EDPB

The EDPB has published a practical roadmap for organisations seeking to transfer personal data internationally in a compliant manner in the wake of *Schrems II*. This roadmap sets out six recommended steps:

1) Map all transfers of personal data

As a first step, organisations should identify and catalogue all of their international personal data transfers. The EDPB used this opportunity to remind organisations that remote access to personal data, or the cloud storage of personal data, may constitute transfers to be included in this exercise.

2) Verify that this personal data is being transferred in a compliant manner

Once the data flows have been catalogued, the tool (for example, SCCs) that each transfer relies upon must be identified.

An international transfer of personal data should not proceed without an appropriate transfer tool in place. The transfer tools available are (i) an adequacy decision in respect of the recipient country made under Article 45 of the GDPR, (ii) one of the mechanisms provided for under Article 46 of the GDPR, including SCCs and Binding Corporate Rules, or (iii) one of the derogations provided for in Article 49 of the GDPR (such as public interest).

3) Assess if there is any law or practice in the receiving country that would limit the effectiveness of the

safeguards created by the transfer mechanism in use

The third step requires organisations to assess each transfer tool, and identify – on a practical level – if each tool being relied upon protects personal data to the level required by the GDPR.[3]

Of principal concern, per the EDPB, is the existence of "anything in the law or practice of the [receiving country] that may impinge on the effectiveness of the appropriate safeguards" being relied upon. *Schrems II* highlighted the difficulties posed by the US' mass surveillance programmes in this regard. If a transfer tool is unable to provide an adequate level of protection, despite otherwise being valid, it should not be used alone as a means of transferring personal data outside of the EU.

Where an assessment is required, the EDPB recommends that this should be based on an objective review of the receiving country's legislation or, if this is not possible, "other relevant and objective factors". This assessment should not take into account any subjective factors, such as the type of data being transferred. If the receiving country's laws do not allow for personal data to be protected, then further action, as detailed in step 4 below, will be required.

It is possible that a country's legislation empowers national security agencies to access personal data. If this is the case, the assessment should consider (i) the extent to which these powers are limited to what is necessary or proportionate in a democratic society, or (ii) if they breach EU standards.[4]

Any such assessment will be a complex undertaking. Helpfully, however, the EDPB does provide practical and positive recommendations in this regard. In particular, the EDPB notes that:

1. it is possible to conclude following an assessment that any potential interference permitted by a country's laws will be limited to a similar degree to that to level of potential interference allowed under the GDPR; and
2. the existence of a comprehensive data protection law, or an independent data protection authority, can indicate that a country's potential interference with personal data protections can be considered proportionate.

This is a pragmatic approach from the EDPB and seems to be designed to empower organisations to make positive decisions as to the ability to transfer personal data internationally, where appropriate.

In any event, the assessment should be clearly documented and undertaken carefully. The EDPB notes that organisations will be held accountable for the decisions made based on the assessment.

4) Identify and adopt any additional measures as necessary to bring the level of protection for this data to the level required by the GDPR

It is possible that a company concludes that the transfer tool they intend to rely on, by itself, will not provide the required level of protection for personal data. This may be the case with transfers to the US in light of *Schrems II*. The EDPB has however provided companies with suggestions as to how supplementary measures can be used to continue data transfers even if the tool for transfer alone is insufficient.

These supplementary measures are categorised as being of a technical, contractual, or organisational nature. All three, when used in combination, are likely to be most effective in ensuring compliance with the GDPR.

The technical measures suggested by the EDPB include:

- "State-of-the-art" encryption;
- Pseudonymisation, where the personal data being transferred is altered such that an individual can no longer be identified without further information; and
- Split processing, where the personal data is segmented and provided to separate parties, such

that no one party can identify an individual from the data it receives.

The contractual measures listed by the EDPB include imposing obligations on recipients of the personal data to implement appropriate technical measures, or a requirement for relevant legislative developments within the recipient country to be brought to the attention of the data exporter by the recipient.

Organisational measures relate to internal policies or methods, intended to improve a company's awareness of the risks present in transferring personal data outside of the EU.

It is important to note that these supplementary measures must be capable of ensuring, in conjunction with a transfer tool, that the level of data protection provided will meet the level required by the GDPR. If this is not the case then the transfer should not proceed.

5) Take formal procedural steps if required

Where supplementary measures are identified and implemented, certain formalities may need to be completed. These should be completed prior to any international transfer of personal data.[5]

6) Periodically re-evaluate the level of protection these transfers enjoy

Finally, once this process has been concluded, organisations should ensure that they monitor any developments in countries where personal data has been transferred. In the event there are any developments, these six steps should then be re-visited to ensure continued compliance with the GDPR.

Draft SCCs Published by the European Commission

Seemingly drafted with the EDPB guidance in mind, the European Commission has proposed a new set of SCCs. This document, currently published in draft form, is open for consultation until 10 December 2020. It is currently unclear when the final version of the revised SCCs will be published.

Importantly, and not entirely in response to *Schrems II* or the EDPB guidance, these draft SCCs represent a clear attempt by the European Commission to provide as practical a set of SCCs as possible. For example, the draft SCCs:

1. Cater for international data transfers from a data processor to another data processor, a long overdue development;
2. Set out a new modular approach, allowing for parties to use one single template document to govern transfers from (i) controller-to-controller, (ii) controller-to-processor, (iii) processor-to-processor and (iv) processor-to-controller; and
3. Reference the need for parties, using whichever module, to assess what constitutes an "appropriate level of security" for a transfer, account for the risks involved in a transfer, and then undertake due consideration of the technical measures that would be appropriate to safeguard a transfer.

In perhaps one of the more significant concessions to businesses put into some difficulty by *Schrems II*, the European Commission's draft measures currently provide for a year's grace period to implement these new clauses. This would give organisations time to transition from the previous form of SCCs (subject to implementing any required supplementary measures in the meantime) to the new version, whenever these are finalised.

Conclusion

In the face of the uncertainty that *Schrems II* created, it is to be welcomed that the EDPB and European Commission have sought to provide practical guidance to organisations. This uncertainty has been

compounded by the impending end of the Brexit transition period on 31 December 2020, following which personal data transfers from the EU to the UK will need to rely on an effective and reliable transfer tool. The finalisation of the new SCCs will allow for greater stability in that regard. It is a fact that many businesses rely on international personal data transfers for various reasons, and a recognition that these should be facilitated as far as possible is a positive step.

Organisations now face the task on implementing the EDPB's recommendations, which is where their utility and practicality will really be tested.

---

[1] Case C-311/18, available here.

[2] The EDPB is the body within the EU tasked with ensuring that data protection rules are applied consistently within the bloc.

[3] It should be noted that, where the transfer of personal data relies on an adequacy decision, no further steps need to be taken in this regard, apart from ensuring on a periodic basis that this decision is still in force. This is because, unlike other transfer mechanisms, an EU adequacy decision in effect states that there are no laws or practices that would undermine data protection rights in that jurisdiction.

[4] Greater guidance is available from the EDPB, available here. Broadly, EU standards are as follows:

- Processing should be based on clear, precise and accessible rules.
- Necessity and proportionality with regard to the legitimate objectives pursued need to be demonstrated.
- An independent oversight mechanism should exist.
- Effective remedies need to be available to the individual.

[5] Such formalities include, for example, where parties seek to deviate from the SCCs, or the technical measures that are required in some way contradict the SCCs. In such an instance prior approval from the appropriate Data Protection Authority would be required before any international transfer of personal data occurs.

Contact Us

Kelly Hagedorn

khagedorn@jenner.com | Download V-Card

David P. Saunders

dsaunders@jenner.com | Download V-Card

Matthew Worby

mworby@jenner.com | Download V-Card

Meet Our Team

Practice Leaders

David Bitkower

Chair

dbitkower@jenner.com

Download V-Card

David P. Saunders

Co-chair

dsaunders@jenner.com

Download V-Card