Intellectual Property & Technology Law Journal

Edited by the Technology and Proprietary Rights Group of Weil, Gotshal & Manges LLP

VOLUME 33 • NUMBER 3 • MARCH 2021

Schrems II: European Data Protection Board Data Transfers Guidance

Karen L. Neuman, Paul Kavanagh, Dylan Balbirnie, and Madeleine White

Months after the landmark *Schrems II* decision of the Court of Justice of the European Union ("CJEU"),[1] the European Data Protection Board ("EDPB") has issued its recommendations on "supplementary measures" to help protect personal data transferred from the European Economic Area ("EEA") to third countries and ensure compliance with the General Data Protection Regulation ("GDPR") (the "Recommendations").[2] The decision invalidated the EU-U.S. Privacy Shield and particularly focused on the use of other transfer tools such as standard contractual clauses ("SCCs"), ruling that SCCs were valid in principle but that the transfer parties needed to assess whether the law of the destination country ensured adequate protection of the personal data transferred and provide supplementary measures where necessary.

Karen L. Neuman (*karen.neuman@dechert.com*) is global head of privacy counseling and a partner in Dechert LLP's Privacy and Cybersecurity practice providing strategic advice to clients on all matters involving data privacy and protection across industries, with particular focus on the application of emerging technologies on data driven products and services. **Paul Kavanagh** (*paul.kavanagh@dechert.com*) is a partner in the firm's Privacy and Cybersecurity practice advising on commercial privacy matters and cybersecurity risks and incidents. **Dylan Balbirnie** (*dylan.balbirnie@dechert.com*) is an associate at the firm advising on the intersecting patchwork of global laws that govern privacy and data security. **Madeleine White** (*madeleine.white@dechert.com*) is an associate at the firm focusing her practice on privacy matters including assisting businesses with their compliance obligations under UK and EU data protection legislation.

KEY TAKEAWAYS

- Mapping is key: the Recommendations highlight the importance of knowing your data transfers and transfer tools relied upon. Organizations should have already conducted data mapping for their GDPR compliance programs (with periodic updates to reflect changes to data activities and legal developments) which will set out their data flows and transfers. For those still working on this mapping, others whose data flows are subject to regular change and those dealing with the aftermath of Brexit and the EU-UK Trade and Cooperation Agreement, this mapping takes on renewed importance.

- Technical measures are your best bet at putting in place supplementary measures appropriate to bring the level of protection of the data transferred up to the EU standard of essential equivalence. Whilst the Recommendations do set out contractual and organizational measures that can

be taken to complement technical measures put in place, they flag that these kinds of measures can only do so much as they cannot bind public authorities in the data importer's country.

- It is still the primary responsibility of the data exporter organization to ensure that the data transferred is afforded a level of protection essentially equivalent to that guaranteed within the EU. Whilst some may be frustrated by the lack of a magic bullet solution from the EDPB which means businesses are still required to undertake a burdensome assessment of the laws of the country of import, the reality is that this is a complex challenge with a political backdrop and for the time being the buck stops with businesses.

- The Recommendations aim at providing a methodology (comprising a series of steps) for data exporters to determine whether and which supplementary measures would need to be put in place in order to ensure that data transferred outside of the EEA is afforded a level of protection "essentially equivalent" to that guaranteed within the EEA. Helpfully, they do include a number of examples.

STEP 1 – MAP YOUR TRANSFERS

The Recommendations point out that before a data exporter can know what steps it needs to take, it needs to know what transfers are taking place. Indeed, a key part of fulfilling obligations under the GDPR principle of accountability requires an exporting organizations to be "fully aware" of all its transfers of personal data to third countries outside of the EEA.

Organizations are reminded that remote access from third countries and/or storage in a cloud located outside the EEA are still considered transfers of personal data. Onwards data transfers, from data processors to sub-processors for example, also need to be taken into account.

As part of the mapping exercise, exporters should verify that the personal data transferred is limited to that which it is necessary to transfer for the relevant purposes. Many organizations will already have conducted data mapping as part of their GDPR compliance programs but for those still working on this, those for whom this is an ongoing exercise given regular changes in data flows and those dealing with the aftermath of Brexit and the EU-UK Trade and Cooperation Agreement, this mapping has renewed importance in the current climate.

STEP 2 – IDENTIFY/VERIFY YOUR TRANSFER TOOL

As a reminder, under the GDPR, personal data may only be transferred outside the EEA (i) if the third country to which the data is to be transferred has been the subject of an adequacy decision; (ii) if appropriate Article 46 safeguards/transfer tools are put in place (e.g., SCCs or binding corporate rules); or (iii) on the basis of certain Article 49 derogations. Of these options, SCCs are the most widely used.

The first thing to check is whether the exporter can rely on an adequacy decision of the European Commission.[3] If so, no further steps in the methodology need be taken although the exporter will still need to monitor whether the decision is revoked or invalidated (as happened with the EU-U.S. Privacy Shield).

The Recommendations then go on to consider Article 46 transfer tools and Article 49 derogations. Although setting these out in this order, the Recommendations go on to say that "if your transfer can neither be legally based on an adequacy decision, nor on an Article 49 derogation, you need to continue with step 3" which covers an assessment of the effectiveness of an Article 46 transfer tool. This suggests that the EDPB had in mind that organizations could consider whether they can make a derogation work before turning to an Article 46 transfer tool. Derogations are supposed to be exceptional in nature, interpreted restrictively and mainly relate to processing activities that are occasional and non-repetitive. From a practical standpoint though, considering whether a derogation can work first does make the most sense.

STEP 3 – ASSESS THE EFFECTIVENESS OF YOUR TRANSFER TOOL

This step 3 was the main concern of the *Schrems II* judgment and one of the more problematic aspects for organizations to deal with in practice. The key thing that the assessment is looking to address is whether the applicable law of the country of import impinges on any of the commitments in the Article 46 transfer tool. In particular, organizations should look at any laws laying down requirements to disclose personal data to public authorities

or granting such public authorities powers of access to personal data. The Recommendations do at least recognize that there may be some level of access but provide that so long as these requirements or powers are limited to what is necessary and proportionate in a democratic society (by reference to EU standards) they may not impinge on the commitments in the transfer tool. To this end, the EDPB has also provided recommendations on the European Essential Guarantees for surveillance measures to assist in conducting an assessment.

The Recommendations suggest that organizations should take into account the following circumstances when considering how the legal framework of the country of import applies to the particular transfer:

- The purposes for which the data are transferred and processed (e.g., marketing, HR, storage, IT support, clinical trials);
- The types of entities involved in the processing (public/private; controller/processor);
- The sector in which the transfer occurs (e.g., adtech, telecommunication, financial);
- The categories of personal data transferred;
- Whether the data will be stored in the third country or whether there is only remote access to data stored within the EU/EEA;
- The format of the data to be transferred (plain text, pseudonymized or encrypted);
- The possibility that the data may be subject to onward transfers from the third country to another third country.

For example, in *Schrems II*, the CJEU held that Section 702 of the U.S. Foreign Intelligence Surveillance Act does not respect the minimum safeguards resulting from the principle of proportionality under EU law and cannot be regarded as limited to what is strictly necessary. Therefore, transfer tools cannot be relied upon unless additional supplementary measures make access to the data transferred impossible or ineffective according to the Recommendations.

If an essentially equivalent level of protection is not ensured, the data exporter needs to move on to step 4.

STEP 4 – IDENTIFY AND ADOPT SUPPLEMENTARY MEASURES

Measures will need to be considered on a case-by-case basis as there will not be a uniform solution for all transfers. The Recommendations provide for three categories of measures (which are in essence those that have been suggested by privacy practitioners since *Schrems II*): technical, contractual, and organizational.

At the outset, the EDPB is at pains to point out that contractual and organizational measures can only go so far as they cannot by their very nature bind public authorities in third countries, however, they can be used to supplement technical measures.

Technical Measures

Unsurprisingly given the CJEU's comments in *Schrems II*, the EDPB's technical examples focus on preventing access to personal data by public authorities in non-adequate third countries. Implementation of one of these technical measures is not a panacea; ultimately the question is still whether the personal data can be afforded an essentially equivalent level of protection once transferred to the third country and so the supplementary measure must bring the level of protection up to this standard, otherwise the transfer must not take place. In practice though, the more measures that are taken the less likely that there will be significant enforcement action or claims.

It should be noted that the Recommendations set out scenarios where the EDPB considers that technical measures could potentially be effective as well as scenarios where the EDPB could not find that any technical measures would be sufficient. The primary distinction centers on the level of access to personal data required in the third country (i.e., does the data importer need access to the personal data in the clear).

Effective Supplementary Measures

Where no access in the clear (i.e., access to the base unencrypted data) is required, for example, where the transfer is for data storage for backup purposes or where the transfer of pseudonymized

data for analysis is sufficient, the EDPB considers that encryption and pseudonymization (as a security measure) can provide an effective supplementary measure. However, the Recommendations do lay down some fairly stringent standards.

For encryption, this covers six features including that the encryption algorithm and its parameterization must conform to the state-of-the-art and be considered robust against cryptanalysis performed by public authorities in the relevant third country, that the encryption algorithm is "flawlessly implemented" by properly maintained software, and sole control of the keys being retained by the data exporter or another entity in the EEA or an adequate country.

For pseudonymization, the additional information that would be required to attribute data to a specific data subject must be held solely by the data exporter in the EEA or an adequate country, disclosure or unauthorized use of that additional information must be prevented by appropriate technical and organizational safeguards, and the exporter must have established by a thorough analysis of the data in question and taking into account any information that the public authorities of the recipient country may possess that the pseudonymized personal data cannot be attributed to a specific person even if cross-referenced with the other information available to the public authority. This latter requirement seems a tall order in many cases.

The examples also include (a) where encrypted data is routed via a third country on its way to another EEA or adequate country (similar encryption standards as described above are to be implemented) which does potentially mean a need for additional safeguards across the board wherever personal data are transferred; (b) protected recipient status of the data importer; and (c) split or multiparty processing.

Scenarios Where There Is No Effective Measure

Importantly, the Recommendations also set out scenarios where the EDPB considers that no measures would be effective, which cover a large proportion of everyday business transfers. These include transfers to cloud service providers or other processors where those parties require access to the personal data in the clear, and remote access to data for business purposes (e.g., HR, marketing assistance).

In these cases it will largely be about limiting risk rather than seeking to achieve full compliance (which the EDPB is effectively saying is impossible) if the exporter feels the transfer is still necessary, by completing the transfers review and assessment and putting in place extra security measures and policies in order to demonstrate that the inherent risks to data subjects are being minimized should a regulator come calling.

Contractual Measures

For contractual measures (to be used in conjunction with technical measures where the concern is access by public authorities in the third country), the Recommendations suggest contractual obligations:

(i) To put specific technical measures in place;

(ii) On the importer to provide information about the level of access by public authorities in its country;

(iii) Certifying the non-existence of back doors or other access methods;

(iv) Reinforcing audit or inspection powers;

(v) Requiring the importer to inform the exporter promptly of any inability to comply with its contractual commitments;

(vi) As to a "warrant canary" method where the importer provides regular notifications that it has received no orders to disclose personal data unless and until one is received;

(vii) To challenge orders for disclosure where possible and minimize the disclosure (similar to confidentiality type obligations) and inform the requesting authority of the incompatibility of the order with the transfer tool; and

(viii) Not to voluntarily disclose data without the data subject's consent, and/or to notify the data subject or any disclosure order, and/or to assist the data subject in exercising their rights or seeking redress.

Organizational Measures

Organizational measures may include internal policies (with clear allocation of responsibilities, reporting channels and standard operating procedures in the event of public authority requests) alongside specific training for relevant personnel, transparency policies, data minimization, and strict security policies and practices.

STEP 5 – IMPLEMENT THE REQUIRED PROCEDURAL STEPS

Exporting organizations will be required to take procedural steps depending on which transfer tool is being used. For example, it may be necessary for an exporting organization to ask the competent authority to review their supplementary clauses within the SCCs if those clauses contradict any of the existing provisions.

STEP 6 – MONITOR AND REVIEW

The EDPB recommends that exporting organizations review, on a regular basis, any legal or regulatory developments affecting the third country where the importing organization is located.

FINAL COMMENT

The Recommendations were open for public consultation until November 30, 2020 and whilst there will likely be pressure from businesses to relax the guidance in certain areas, it seems unlikely that any wholesale changes will be made. In the teeth of a challenging political backdrop, the EDPB Recommendations are an attempt to provide real examples and options to help businesses maneuver through these requirements. However, they are unable to provide a magic bullet practical solution to the challenges created by *Schrems II*. Ultimately, it remains the primary responsibility of the data exporter to ensure that data transferred to a third country is afforded a level of protection essentially equivalent to that guaranteed within the EU.

Notes

1. *http://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=9777395.*
2. Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, *available* at *https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/recommendations-012020-measures-supplement-transfer_en*; and Recommendations 02/2020 on the European Essential Guarantees for surveillance measures, *available at https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_en.*
3. Adequacy decisions - How the EU determines if a non-EU country has an adequate level of data protection, *available at https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.*