New EDPB Guidance on International Transfers Following *Schrems II*.

November 2020

On November 10, the European Data Protection Board ("EDPB") released its "Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data" (the "Guidance").[1] The Guidance addresses the important topic of how data exporters can ensure the lawfulness of transfers to countries outside of the EEA, following the Court of Justice of European Union's ("CJEU") judgment in *Schrems II* (see our previous summary of that judgment here).

In this alert, we summarize the Guidance and provide the following key takeaways:

- Data mapping – or in this case, *transfer mapping* – continues to be an important and fundamental step towards privacy compliance.
- Data exporters must take an active and ongoing role in reviewing surveillance regimes and other laws and practices that may impact data protection when transferring personal data outside the EEA.
- The EDPB's examples of supplemental measures are non-exhaustive and include technical, organizational and technical measures; however, many of these measures are difficult to implement, impractical and generally ineffective.
- Many transfers to the U.S. and other countries engaged in mass surveillance will specifically require the implementation of effective technical measures such as end-to-end encryption.
- Transfer compliance is not a matter of having "magic words" in a contract.

I. Background

The EU's General Data Protection Regulation ("GDPR") restricts transfers of personal data from the EU to third countries. The GDPR allows international transfers only if the European Commission has determined in an "adequacy decision" that a third country provides adequate safeguards to protect the privacy rights of data subjects in the EU or if the transferring parties have implemented approved "transfer tools" (e.g., Standard Contractual Clauses ("SCCs"), Binding Corporate Rules, etc.) to ensure equivalent protections for the transferred personal data.

In *Schrems II*,[2] while invalidating the U.S.-EU Privacy Shield, the CJEU confirmed the validity of SCCs and other transfer tools. However, the CJEU clarified that data exporters,

Authors

Elizabeth (Liz) Harding
303.583.8228
eharding@polsinelli.com

Steven A. Hengeli, Jr.
816.360.4392
shengeli@polsinelli.com

Hale H. Melnick
312.463.6207
hmelnick@polsinelli.com

POLSINELLI

[1] European Data Protection Board, *Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data* (adopted on 10 November 2020), https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf.

[2] *Data Protection Commissioner v. Facebook Ireland LTD, Maximillian Schrems*, C-311/18 [hereinafter, "Schrems II"].

even when implementing approved transfer tools, remain accountable for ensuring that the laws and practices in a third country (e.g., relating to surveillance) do not impinge on the effectiveness of the implemented transfer tools. The CJEU suggested that data exporters may need to implement supplemental measures in addition to an GDPR-approved transfer tool, but it did not provide any guidance on when and how to implement such supplemental measures.

The Guidance picks up where the CJEU left off. Specifically, the Guidance lays out a road map for data exporters to follow to (i) determine whether transfers from the EEA to third countries provide adequate safeguards for the protection of personal data under the circumstances and (ii) if not, the kinds of supplemental measures that data exporters – with assistance from data importers – can implement to help shore up protection.

II. The EDPB's Recommended Process.

The recommendations, broken down into six "steps," aim at providing a methodology for data exporters ("you") to determine whether and which additional measures would need to be put in place for their transfers.

- **Step 1: Know your transfers**

Know your transfers (i.e., ensure that you are fully aware of your transfers by recording and mapping them, including onward transfers) so that the transfers are afforded an essentially equivalent level of protection wherever it is processed. Verify that the personal data you transfer is adequate, relevant and limited to what is necessary in relation to the purposes for which it is transferred to and processed in the third country. In performing this mapping exercise, it is important to include any remote access from a third country and/or storage in a cloud situated outside the EEA.

- **Step 2: Identify the transfer tools you are relying on.**

Identify the transfer tool your transfer relies or will rely on (e.g., adequacy decision, SCCs, Binding Corporate Rules, etc.). Adequacy decisions do not require any supplementary measures as long as the decision is still in force. However, because the other transfer tools are of a contractual nature, they may require supplemental measures. Note that if you rely on the Standard Contractual Clauses, the European Commission recently issued a new version of the Clauses that is currently undergoing a feedback period.

- **Step 3: Assess whether the transfer tool you are relying on is effective in light of all circumstances of the transfer.**

Assess whether there is anything in the law or practice of the third country that may impinge on the effectiveness of the appropriate safeguards of the transfer tool you are relying on in the context of your specific transfer. Your assessment should be primarily focused on third country legislation that may undermine its level of protection and all of the actors participating in the transfer (e.g., subprocessors in the third country). Reference should be made to the EDPB European Essential Guarantees, including the EDPB's recommendations on surveillance measures.[3] Special consideration should be given when the legislation governing the access to personal data by public authorities is ambiguous or not publicly available. You should not rely on subjective factors such as the likelihood of public authorities' access to your personal data in a manner not in line with EU standards. You should conduct this assessment with due diligence and document it thoroughly, as you will be held accountable to the decision you may take on that basis.

- **Step 4: Identify and Adopt Supplementary Measures.**

If your assessment in Step 3 concludes that your Article 46 transfer tool is ineffective, then the data exporter – with appropriate collaboration from the data importer – should implement "supplementary measures" to help address the gap. Factors to

[3] *See* EDPB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures, 10 November 2020, https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations022020-european-essential_en.

generally consider when determining the efficacy of supplemental measures on a case-by-case basis include format of the data (plain text v. pseudonymized or encrypted); nature of the data; length and complexity of processing workflow (e.g., how many controllers/processors are involved; duration of processing); and the possibility of onward transfers.

The EDPB provides much-anticipated and non-exhaustive examples of supplementary measures and guidance on scenarios in which these supplemental measures are most likely to be effective. We summarize those measures in Part III, below.

Supplemental measures include technical, contractual and organizational measures. ***However***, for data importers in the United States where the CJEU has already concluded in *Schrems II* that mass surveillance poses a data protection problem, it is important to note the caveat provided by the EDPB: "contractual and organizational measures alone will generally not overcome access to personal data by public authorities . . . in particular for surveillance purposes." This means that, prior to exporting personal data to the U.S. (or other countries with surveillance regimes not in line with EU data protection principles), data exporters will likely need to implement supplemental technical measures to prevent access by governmental authorities. Data exporters cannot rely on changes to contracts or organizational policies alone.

- **Step 5: Take Any Formal Procedural Steps.**

In this step, the EDPB addresses any procedural steps that a data exporter must take such as seeking approval from a supervisory authority before transferring the personal data. The procedural steps depend on the transfer tool used. Generally, no formal steps are needed if using unmodified SCCs. In contrast, if you modify SCCs or implement any supplemental contractual measures that conflict with SCCs, then you must seek authorization from the supervisory authority. The EDPB indicated that *Schrems II* also impacts Binding Corporate Rules and ad hoc clauses, but that it would provide additional guidance on those topics at a later date.

- **Step 6: Re-Evaluate at Appropriate Intervals.**

The obligation to ensure adequacy is an ongoing obligation. A data exporter should monitor for any changes to the circumstances relevant to their assessment. The EDPB does not specify a time period for periodic re-evaluation. Every data exporter should implement a process to stay up-to-date on material changes in the countries in which personal data is imported, including any onward transfers, and to implement update its assessment accordingly.

III. The EDPB's Examples of Supplemental Measures

The EDPB's examples of supplemental measures are non-exhaustive. The EDPB categorizes the supplemental measures as technical, contractual or organizational. In the table below, we summarize the EDPB's examples (in the first column), and highlight key limitations in the second column.

Technical Safeguards

Supplemental Measure	Key Limitations
A data exporter uses a hosting service provider in a third country to store personal data, e.g., for backup purposes	The EDPB lays out many conditions for effectiveness – including encryption prior to the transfer, the use of state of the art encryption and control of encryption keys in the EEA or an adequate jurisdiction.
Transfer of Pseudonymized Data	The EDPB lays out many conditions for effectiveness. Prior to transfer, personal data must be effectively pseudonymized—rendered such that data cannot be attributed to a specific data subject without the use of additional information, which includes additional information likely available to a public authority. Any additional information held by the data exporter must remain in the EEA or an adequate jurisdiction and outside the reach of the data importer.
Encrypted Data Merely Transiting Third Countries	This measure is limited to situations where personal data is merely transiting through third countries. Even in such limited circumstances, the EDPB raises many considerations for implementing an effective form of transit encryption, taking into account the vast resources that public authorities may have to circumvent or break encryption.
The Transfer Recipient is Specifically Protected by that Country's Laws	Aside from requiring the laws in the third country to specifically protect the recipient (e.g., a law relating to professional secrecy) and all data held by the recipient for a given purpose, this measure also requires that any transferred data is protected through state-of-the-art end-to-end encryption with due protection for the encryption keys secured against use or disclosure.
Split or Multi-Party Processing	This measure is available where the parties are able to split personal data for processing using secure multi-party computation where each processor (and any potential public authority accessing the data) only has access to data that can no longer be interpreted or attributed to a specific data subject without the use of additional information.

In addition the limitations discussed above (and additional limitations mentioned in the full Guidance), these technical measures are only available where there is no need to view or access data "in the clear" in the third country. The EDPB specifically notes that these measures are not effective for cloud services that need to process decrypted data or where remote access is needed for business purposes in a third country.

Contractual Safeguards

This section summarizes the EDPB's example contractual measures. Each of these measures reflects an obligation to be placed in the agreement between the data exporter and the data importer.

Supplemental Measure	Key Limitations
Obligation to use specific technical measures to protect personal data.	This is a contractual term where the parties agree to implement technical measures. While this is a useful (and recommended) way to document the use of technical measures, it still requires the parties to be able to implement technical measures in an effective manner.
Transparency obligations, including: ▪ Obligation for data importer to provide data exporter with information on access to data by public authorities (e.g., through a structured questionnaire). ▪ Representations and warranties from the importer that no backdoors will be implemented enabling access to personal data ▪ Provide updates on legal, policy or other developments impacting a previous adequacy assessment ▪ Warrant canary, where the data importer provides regular messages (using a private key to help prevent falsified messages) informing the data exporter that it has received no order to disclose personal data.	These types of contractual terms help ensure that the data exporter has the information that it needs in order to comply with its obligation to assess any data protection issues in the data importer's jurisdiction on a case-by-case and ongoing basis. However, these transparency obligations, even where fully implemented by the data importer, do not help a data exporter overcome those limitations where applicable.
Obligations to take specific actions, including: ▪ Reviewing the legality of any order to disclose data, challenging the order if it concludes there are grounds to do so, seeking interim measures to suspend the order during the challenge, and minimizing the amount of data ultimately provided under the order to the extent possible. ▪ Informing the public authority of the incompatibility of the order with the transfer tool, and notifying the data exporter of any such order as soon as possible	The effectiveness of these measures are dependent on the laws of the country of the data importer, which are likely to be the very source of the problem leading to the implementation of these supplemental measures. For example, the EDPB notes that a clause requiring the data importer to object to an order "will always offer a very limited additional protection as an order to disclose data may be lawful under the legal order of the third country, but this legal order may not meet EU standards."
Obligations to empower data subject rights, including: ▪ Requiring consent of the data subject or the data exporter for any access to personal data transferred in plain text; ▪ Notifying the data subject of the public authority's request or of the data importer's inability comply with its contractual commitments; or ▪ Assisting the data subject with exercising his or her rights in the third country.	Aside from practical difficulties (e.g., whether the data importer is well positioned to directly communicate with the data subject), these contractual measures are ineffective if the applicable law in the data importer's jurisdiction prevents the data importer from notifying the data subject (or, as applicable, the data exporter) of the request. Further, these measures are also of limited effectiveness where the data subject – even with knowledge of the request – has limited recourse under applicable law to challenge the request.

Organisational Measures

This section summarizes the EDPB's examples of organisational measures. Organisational measures consist of internal policies, organisational methods and standards, that controllers and processors could apply to themselves and impose on the importers of data in third countries.

Supplemental Measure	Key Limitations
Implement policies to govern transfers of personal data and processes for responding to requests from public authorities.	The EDPB notes that this measure is only effective in helping prevent disclosures where a public authority's request is *compatible* with EU law.
Implement transparency and accountability measures, including: ▪ Document requests from public authorities, and making such documentation available to data exporters (who, in turn, should provide to data subjects); and ▪ Publication of transparency reports or summaries regarding governmental requests.	Organisational measures involving transparency are limited to the extent that applicable law does not permit the data importer to provide such transparency.
Implement data access controls and data minimization measures; provide timely information concerning transfers to a DPO (or legal/audit teams, as applicable); and adopt strict data security and privacy policies based on EU certification or codes of conduct or international standards (ISO norms) and best practices (e.g., ENISA), taking into account the state of the art and likelihood of attempts from public authorities to access it.	All of these measures are recommended practices for any processing of personal data – whether or not involving an international transfer. Therefore, it is unclear how helpful these measures are to solve any data protection concerns where a transfer to a data importer is necessary and otherwise supported by data minimization principles.