Arnold & Porter

November 24, 2020

# How to Handle Schrems II: European Data Protection Board Issues New Guidance on Cross-Border Transfers of Personal Data

Advisory

By Ronald D. Lee, Alexander Roussanov, Jami Mills Vibbert, Nancy L. Perkins, Jason T. Raylesberg

On November 11, 2020, the European Data Protection Board (EDPB) published new guidance on cross-border transfers of personal information in light of the July 2020 judgment of the Court of Justice of the European Union (CJEU) in Case C-311/18 *Data Protection Commission vs. Facebook Ireland and Maximillian Schrems* (*Schrems II*). This judgment, which invalidated the EU-US Privacy Shield Framework (European Commission Decision (EU) 2016/1250) (Privacy Shield), removed a key mechanism for transfers of personal data from the European Union (EU) to the United States in compliance with the General Data Protection Regulation (GDPR). The new draft EDPB guidance (Recommendations)[1] adds prescriptive detail to the Frequently Asked Questions (FAQs) issued by the EDPB on July 23, 2020,[2] which explained the significance of *Schrems II* but offered little practical guidance for the thousands of companies engaging in transfers of personal data from the EU to the United States on a daily basis. The Recommendations remain open for public consultation through November 30, 2020.

In light of the Recommendations, as summarized below, data exporters in the EU must undertake to understand the risks of, and document their risk-mitigation measures for, transfers of personal data to the United States (and other countries that have not received an "adequacy" determination from the European Commission). More than anything, the EDPB seems to want data exporters to "think about it." As with other data privacy assessments, the key is to understand the risk and do something (or some things) to mitigate that risk. And data importers wishing to continue the free flow of data must be ready to help. We would suggest updating your records of processing activity to account for this new assessment of data transfers.

## Background

The Privacy Shield, a framework instituted by agreement between the European Commission and US Department of Commerce, provided a mechanism for the transfer of personal data from the EU to the United States in compliance with the GDPR. Under Article 45 of the GDPR, such transfers may not be made absent the imposition of special requirements on the recipient of the data in the United States (data importer), because, according to the European Commission, the United States fails to provide "adequate" protection for personal information—i.e., the privacy laws and regulations of the United States and its states fail to protect personal data at a level comparable to that of the GDPR. Article 46 of the GDPR recites the options for such special requirements (appropriate safeguards), including government-to-government agreements such as the Privacy Shield that prescribe data protection mandates, as well as Standard Contractual Clauses (SCCs) and Binding Corporate Rules (BCRs), which do the same via contractual obligations or internal rules and standards.

In *Schrems II*, the CJEU found the Privacy Shield was not an "appropriate safeguard" for Article 46 purposes, on the ground that, even if the data importer adhered to all the Privacy Shield requirements, there was still a risk that the imported personal data might be obtained or accessed by the United States government. With respect to SCCs and BCRs, the CJEU indicated that these too would be insufficient absent "supplementary measures" to ensure adequate protection for personal data transferred to the United States, for the same reason. But the CJEU provided scant detail in *Schrems II* on what such supplementary measures might look like.

The Recommendations serve to help fill the gap in the *Schrems II* decision with respect to practical implementation of

sufficient "supplemental measures." The Recommendations set forth a six-step process for data exporters, in collaboration with data importers where appropriate, to identify the need for and to adopt supplementary measures as needed. While the Recommendations include examples of a number of scenarios where supplementary measures may be effective, the EDPB acknowledges that there will be situations where supplementary measures will not be sufficient to ensure compliance. In such cases, data transfers to third countries should be prohibited.

## The EDPB's Six-Step Process for Determining Supplementary Measures

### Step 1: Know your transfers

First, data exporters must fully record and map out all of their transfers. To satisfy this complex step, data exporters must also map any onward transfers, e.g., transfers of data from one processor to a sub-processor in another third country. The EDPB requires that processors and controllers verify that the data transferred 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 accordance with the GDPR principle of data minimization. Moreover, data exporters must map instances of remote access from a third country (e.g., in IT support situations) and/or storage in a cloud located outside of the European Economic Area (EEA).

### Step 2: Identify the transfer tools you are relying on

Second, data exporters must verify the transfer mechanism upon which they will rely. For transfers to the United States, other than in the relatively rare circumstance where one of the "derogations" outlined in GDPR Article 49 applies (e.g., where a data subject consents to a transfer to the United States), the transfer mechanism will be SCCs, BCRs, or (less likely) ad hoc contractual clauses.

### Step 3: Assess whether the GDPR transfer tool you are relying on is effective in light of all circumstances of the transfer

If a data exporter has identified an GDPR transfer tool, it must determine whether that transfer tool is actually effective in practice. For example, although a data importer may agree to an SCC, the laws or practices of the country of that data importer (e.g., the United States) may impede the effectiveness of the safeguards of the SCC. The data exporter is therefore required, in collaboration with the data importer, to undertake a comprehensive analysis of the importer's country's laws and practices to determine whether impediments do in fact exist. The Recommendations list a number of factors applicable to this analysis, but foremost among them are the EDPB's "European Essential Guarantees" set forth in draft Recommendations 2/2020 that were also published on November 11, 2020 and submitted for public consultation open through November 30, 2020. These European Essential Guarantees provide a framework for evaluating whether public authorities in a third country, such as national security agencies and law enforcement authorities, may unjustifiably interfere with the data being transferred. According to the EDPB, respecting these Essential Guarantees will ensure that the power granted to these public authorities will not "go beyond what is necessary and proportionate in a democratic society." The four European Essential Guarantees are as follows:

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

If, upon completing this analysis, it is determined that the data importer cannot comply with its obligations under a particular GDPR transfer tool in light of a third country's legal order as applied to such transfer, then the GDPR transfer tool is not considered to provide an adequate level of protection and the data exporter must either implement effective supplementary measures or not transfer personal data at all.

### Step 4: Adopt Supplementary Measures

Data exporters who determine under Step 3 that a GDPR transfer tool is not effective must then assess, in collaboration with the data importer as appropriate, whether any supplementary measures exist that can be implemented to provide sufficient personal data protection. Although supplementary measures may be contractual, technical, or organizational in nature, the Recommendations note that "contractual and organizational measures alone will generally not overcome access to personal data by public authorities of the third country (where this unjustifiably interferes with the data importer's obligations to ensure essential equivalence)." There therefore will be situations where only *technical* measures can be deemed effective to shield personal data from access by public authorities, although contractual or organizational measures may "complement technical measures and strengthen the overall level of protection of data."

In an Annex to the Recommendations, the EDPB provides a non-exhaustive list of potential supplementary measures that would be sufficient to provide adequate data protection, including:

1. Technical measures:
    1. **Encryption**. State-of-the-art encryption for data both in transit, including transit through a non-destination country, and held in storage by a destination country, may be an effective supplementary measure provided certain conditions applicable to each scenario are met. For example, encryption is considered an effective supplementary measure where a data exporter uses a hosting service provider in a third country to store personal data (e.g., to store files on a website for backup purposes), provided a number of conditions are satisfied, including that the personal data is processed using strong encryption prior to transmission and that the encryption algorithm is flawlessly implemented.
    2. **Pseudonymization**. As long as particular conditions are met, pseudonymization of personal data may be an effective supplementary measure. This would allow, for example, a data exporter to transfer personal data it has already pseudonymized to a third country for research purposes. The limiting conditions include the requirement that any additional, non pseudonymized information be held exclusively by the data exporter and kept separately in the EEA, or in a country that enjoys an adequacy designation.
    3. **Split or multi-party processing**. Again subject to certain conditions, another effective supplementary measure may be implemented by a data exporter who, prior to transmission of data, splits personal data in a manner such that no part of the data an importer receives will permit reconstruction of the personal data. Among the limiting conditions for this measure is that each piece of data must be transferred to a separate processor in different jurisdictions.

    The Annex also identifies several scenarios where technical measures would *not* provide an essentially equivalent level of protection for data transferred to a third country. For example, the Annex states that there is currently no effective technical measure (including implementation of *both* transport and data-at-rest encryption) to adequately protect a data subject, where the following circumstances occur:

    (i) a data exporter processes personal data using a cloud service provider or other processor according to its instructions in a third country;

    (ii) a controller transfers data to such cloud service provider or other processor;

    (iii) the processor must access the data "in the clear" to execute the designated task; and

    (iv) the power granted to public authorities of the third country to access the transferred data is outside of the bounds of what the EDPB considers "necessary and proportionate in a democratic society."

2. Contractual measures

    The Recommendations also describe a number of additional contractual measures that may be effective, including:

    1. **Providing for the contractual obligation to use specific technical measures**. The EDPB notes that these measures could be effective where the data exporter has determined that technical measures are needed, and those measures are then provided in a legal form to ensure the importer's compliance with the required measures.
    2. **Transparency obligations**. A number of potential contractual measures involving transparency could serve to protect personal data. For example, the data exporter could add provisions to a contract requiring the data importer to undertake its best efforts to provide information (e.g., in the form of structured questionnaires) on the access to data by public authorities, such as information on the laws in the third country that permit public authorities to access the personal data being transferred. The data exporter also could add a requirement for the data importer to certify, among other things, that it has not intentionally created any back doors or similar programming that could be used to access the data. In addition, contracts could include provisions for inspection authorities selected by

the exporter to rapidly conduct audits of the data processing facilities of the importer to determine whether any personal data has been disclosed to public authorities.

3. **Obligations to take specific actions**. Contracts also could require importers to review and challenge the legality of any order by public authorities to disclose data or to inform the requesting public body that such order does not comport with the safeguards included in the GDPR transfer tool being used.

4. **Empowering data subjects to exercise their rights**. Especially in circumstances where public authorities request data importers to cooperate voluntarily, it might be necessary to include a contractual provision that conditions access to any personal data transmitted in plain text in the normal course of business on the consent of the data exporter and/or subject. Alternatively, contracts could require the importer and/or exporter to provide notice to the data subject upon receiving a public authority's request for data (although the Recommendations acknowledge that national regulations and policies may prevent this notification, in which case the exporter and importer could commit to informing the data subject once the restrictions on data disclosure are lifted and to make best efforts to obtain permission to disclose), and require the data exporter and importer to provide legal counseling as necessary to help data subjects exercise their rights in the destination country.

3. Organizational measures

Recognizing that organizational measures may provide consistency in protecting personal data and that organizational measures may improve exporters' awareness of risk, the Recommendations identify the following four categories of such measures:

1. **Internal policies for governance of transfers**. Particularly helpful for groups of companies, data exporters should adopt internal policies that clearly set forth responsibilities for data transfers, reporting channels and standard operating procedures.

2. **Transparency and accountability measures**. Among other things, data exporters should document requests for access received from any public authorities, and periodically publish transparency summaries on governmental requests.

3. **Organization methods and data minimization measures**. Confidentiality policies should be adopted and enforced through disciplinary measures. Additionally, data exporters should periodically perform audits.

4. **Adoption of standards and best practices**. Along with confidentiality policies, it is recommended to impose strict data security policies, modeled on European and international standards such as the ISO 8000 norms, and best practices such as those applied by the European Union Agency for Cybersecurity.

5. **Additional organizational measures**. Finally, data exporters should conduct regular reviews of internal policies to evaluate the effectiveness of the above-mentioned measures and should secure commitments from data importers to cease any onward transfer of data to a destination country that fails to provide adequate protection of personal data.

### Step 5: Procedural steps if you have identified effective supplementary measures

Certain procedural steps for implementing supplementary measures may apply, and those steps may differ depending on the type of transfer tool used and the way that tool is utilized. For example, if a data exporter wants to use supplementary measures *in addition* to SCCs, the exporter need not obtain a supervisory authority's authorization to do so, unless the supplementary measures "contradict, directly or indirectly, the SCCs and are sufficient to ensure that the level of protection guaranteed by the GDPR is not undermined." On the other hand, if a data exporter wants to *modify* the SCCs, or the supplementary measure identified contradicts the SCCs, the exporter must obtain a supervisory authority's authorization. The Recommendations are less specific on what procedural steps should be undertaken with respect to BCRs and ad hoc contractual clauses, noting that the "precise impact of the *Schrems II* judgment" is still under discussion with respect to both.

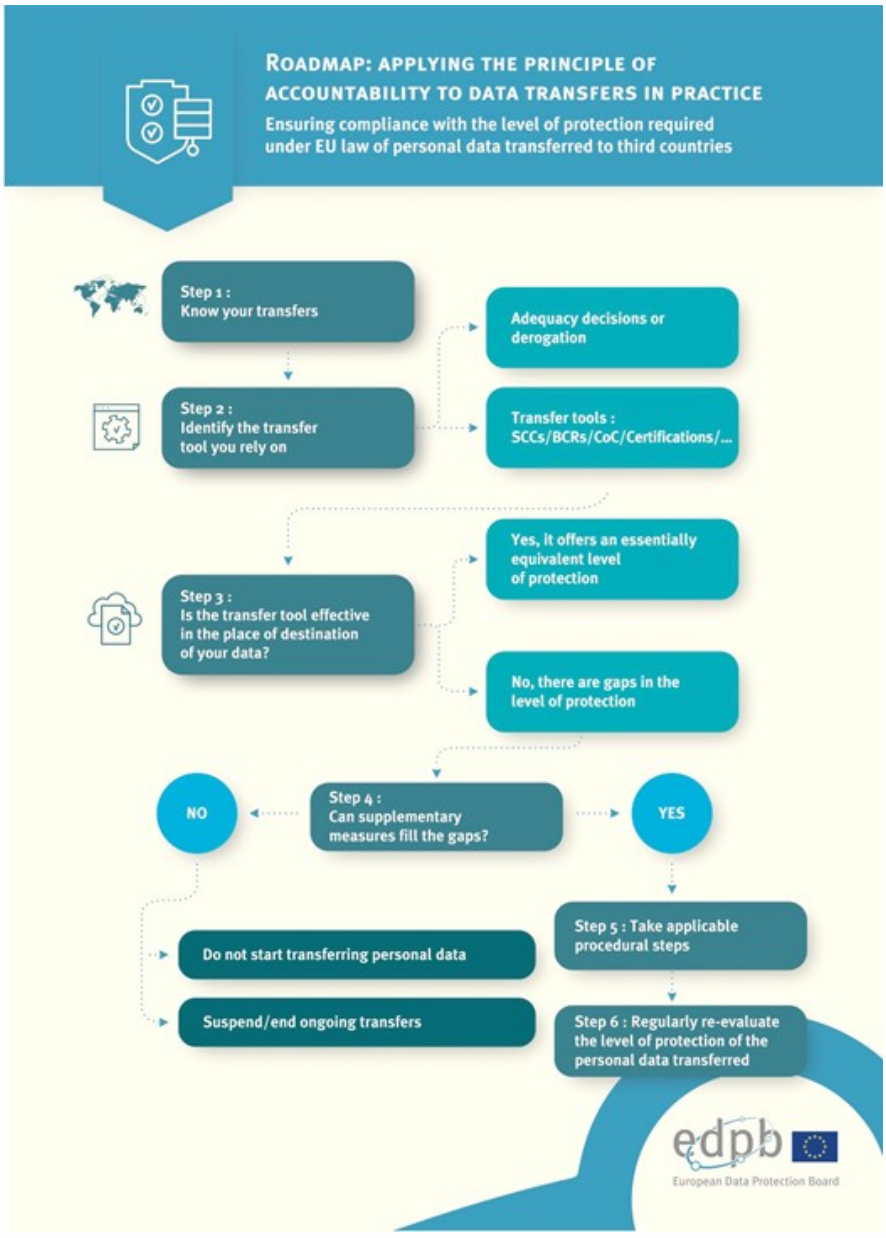
### Step 6: Re-evaluate at appropriate levels

In line with the principle that "accountability is a continuing obligation," the Recommendations suggest that data exporters monitor, in collaboration with data importers as appropriate, any developments in the destination country that might change the conclusion of the original analysis done on the level of protection afforded to the data being transferred. To that end, certain mechanisms should be implemented so that transfers can quickly be terminated or suspended in the event that a data importer cannot abide by its data protection commitments.

## Conclusion

The level of detail involved in each step of this roadmap underscores the complexity of the task data exporters now face in ensuring the legitimacy and legality of international data transfers from the EU. From continuously and meticulously evaluating the laws and practices of destination countries, to considering the sufficiency of particular encryption measures, businesses will be navigating uncertain territory in attempting to overcome the risks identified in *Schrems II* and highlighted in the Recommendations. Although they provide significant and much-needed guidance, the Recommendations leave areas of much uncertainty. As indicated above, the Recommendations at a minimum require data exporters to understand what is happening—to evaluate the data transfers—and to implement supplementary measures designed to address the risks they perceive.

We will continue to monitor developments regarding and modifications to the Recommendations as they are finalized at the conclusion of the public consultation period.



**Source: European Data Protection Board (EDPB)*



[1] "Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data" (Nov. 10, 2020).

[2] *See also* Arnold & Porter's Advisory on the FAQs published on July 30, 2020: *The European Data Protection Board Weights In: What does Schrems II Mean and What Comes Next?*