COSMOS
Navigate the Compliance Universe

CEP Magazine - March 2021
Post-Schrems II EU guidance on data transfer mechanisms-a critique

By Robert Bond

Robert Bond (robert.bond@bristows.com) is Senior Counsel & Notary Public at Bristows LLP in London, UK.

The Court of Justice of the European Union (CJEU) ruling on the validity of the European Commission's standard contractual clauses (SCCs) for international data transfers from the European Union (EU) to third countries was announced on July 16, 2020.[1]

The CJEU declared that the European Commission's decision approving the SCCs was still valid. However, this does not automatically mean that all data transfers made under the SCCs are valid, as the decision emphasizes the obligations on controllers to suspend transfers if the clauses can't be complied with (e.g., government surveillance programs). The CJEU also ruled that the Privacy Shield was invalid.

The key points of the decision include the following:

- Data subjects whose data are transferred to a third country must be given a level of protection essentially equivalent to that guaranteed under the General Data Protection Regulation (GDPR), read in the light of the EU Charter of Fundamental Rights.
- US government surveillance programs and the limitations they are subject to do not meet the requirements of proportionality under EU law and do not grant data subjects actionable rights before the courts against the US authorities.
- The ombudsperson mechanism provided for under the Privacy Shield does not provide a sufficient remedy to make up for this lack of actionable rights, so the Privacy Shield is invalid.
- Regarding transfers under the SCCs, the assessment of the level of protection should consider the protection given by the SCCs and also relevant aspects of the legal system of the destination country when considering access by the public authorities of that third country.
- The SCCs require data exporters and importers to verify, prior to any transfer, whether the level of protection "is respected in the third country concerned." Importers are obliged to notify exporters if they can't comply with the SCCs, and controllers then have an obligation to suspend transfers.
- Data protection authorities should suspend or prohibit transfers of data to a third country if they consider in all the circumstances that the SCCs aren't or can't be complied with in that third country and the protection of the data that is required by EU law cannot be ensured by other means.

On November 11, 2020, the European Data Protection Board (EDPB) published initial guidance on the CJEU's *Schrems II* decision.[2] The guidance was intended to assist controllers and processors in complying with the CJEU's ruling that "data exporters" seeking to rely on the EU's SCCs must (i) conduct a risk assessment of the transfer and, if necessary, (ii) implement "supplementary measures" to protect the data in the recipient country.

The guiding principle in the guidance is that any personal data transferred must be provided with an "essentially equivalent" level of protection, and that it is the responsibility of the controller or processor transferring the data to ensure this essential equivalence is achieved. If essential equivalence cannot be achieved (either through the SCCs alone or through SCCs plus supplementary measures), then the EDPB is clear that the controller or processor cannot transfer the data. Any existing transfers must stop, previously transferred data must be returned or deleted, and no new transfers can take place. The EDPB appeared to leave no scope for a risk-based approach that would consider the specific nature of the data being transferred (e.g., low-risk or publicly available data).

The six-step process

The guidance sets out a six-step process for relying on the SCCs and, in Annex 2, provides examples of "supplementary measures" that could be implemented. This process is extremely burdensome, seeming to disregard the commercial reality that almost all businesses will use some form of cloud-hosted software or services requiring a data transfer.

Note that, in order to meet the GDPR's accountability requirements, each of these steps would need to be documented, and this documentation must be provided to the supervisory authorities on request.

Step 1: Know your transfers

Understand what data you are transferring outside the European Economic Area, including by way of remote access. Perhaps fairly self-evident, but this can be challenging when it comes to onward transfers by processors (to sub, or even sub-subprocessors).

Step 2: Identify your transfer tool(s)

Identify what lawful mechanism you are relying on under GDPR to transfer the data; with Privacy Shield no more, for the overwhelming majority it will be the SCCs. Only a very small number of organizations have binding corporate rules (for which the EDPB indicates more guidance will be forthcoming), and the EDPB again emphasizes that the derogations in Article 49 of the GDPR must be interpreted restrictively.

Step 3: Assess whether the transfer mechanism is effective in practice

Now we come to the crucial question: In practice, is the transferred personal data afforded a level of protection in the third country that is essentially equivalent to the level guaranteed in the European Economic Area? This requires exporters to consider whether anything in the local law potentially thwarts the protection supposedly offered by the SCCs.

The EDPB recommends considering multiple aspects of the third country's legal system but in particular considers the rules granting public authorities rights of access to data. Most countries allow for some form of access for law enforcement and national security, and so the assessment should focus on whether those laws are limited to what is *necessary and proportionate in a democratic society*.

It is difficult to see this assessment being done without instructing local counsel in the third country. The EDPB suggests that, where appropriate, the data importer should provide the relevant resources and information about the laws in their country. But while no doubt many providers will be eager to reassure their customers, they may be equally nervous about giving legal advice.

Disappointingly, the EDPB appears to rule out the possibility of considering the specific circumstances of your

transfer (e.g., the nature of the data) in order to make a risk-based judgment. The guidance is clear that the assessment must only be based on "objective" factors, and exporters should not rely on "subjective ones such as the likelihood of public authorities' access to your data in a manner not in line with EU standards." This feels like a missed opportunity and runs counter to the general risk-based approach advocated throughout the GDPR.

If, after this assessment, you decide the SCCs, notwithstanding the local law, ensure an equivalent level of protection, you can stop there. If, however, you decide that the local law does impinge on the protections granted by the SCCs, you must proceed to Step 4.

Step 4: Adopt supplementary measures

If your assessment of the local law at Step 3 led to the conclusion that SCCs alone would not be sufficient, then you must adopt supplementary measures to protect the data. The EDPB separates potential supplementary measures into three categories: technical, contractual, or organizational.

Annex 2 of the guidance lists examples of the supplementary measures that fall into each of the three categories, but the EDPB's primary focus is clearly on the technical measures, with the EDPB stating that "contractual and organisational measures alone will *generally not* overcome access to personal data by public authorities of the third country."

The *technical measures* are those aimed at preventing access by public authorities altogether, or at least preventing access to data that are identified or identifiable, such as state-of-the-art encryption (where the key is stored by the exporter in the European Economic Area); pseudonymization (where the exporter is comfortable that the data would not be identifiable even if combined or cross-referenced with other data available to the public authority); or splitting data between multiple separate processors in separate jurisdictions.

However, the guidance then gives two examples where it has been *unable* to identify an effective technical measure to protect the data. These are:

1. Sending data to a cloud provider or other processor that requires access to data in the clear. The difficulty faced by a great many providers is that access to the data is inherent to the service they offer, and so encryption at rest is simply not an option.

2. Transfer of data for a shared business purpose: for example, between companies in the same group. Again, the issue here is that the recipient will need the data in a usable format, and so none of the measures above would be viable.

In these circumstances, the exporter can only look to contractual and organizational measures, knowing that the EDPB has some doubts as to how effective they can be on their own.

The *contractual measures* primarily focus on transparency by the importer to the exporter (e.g., certifying that no backdoors have been created, offering enhanced audit rights, and notifying the exporter if it is required to disclose data). The *organizational measures* include internal policies (rather like binding corporate rules), documented processes for responding to disclosure requests, and data minimization.

The challenge with the contractual and organizational suggestions is that they are accompanied in the guidance by very restrictive "conditions for effectiveness," which, in practice, seem unlikely to be met in any country that did *not* satisfy the essential equivalence test in Step 3. For example, a great many disclosure orders will prohibit the recipient from disclosing the existence of the order, cutting across any transparency commitments in a contract. Given, however, the absence of technical measures for the two scenarios listed above, many exporters will be left with little option but to implement all the contractual and organizational measures they can and hope

for the best.

Step 5: Procedural steps if you identified any supplementary measures

This step is only applicable if your supplementary measures contradict the SCCs (which hopefully they won't), and so it seems a bit of a red herring. It is, however, the section of the guidance where the EDPB suggests they may add more requirements to the binding corporate rules in due course.

Step 6: Reevaluate at appropriate intervals

Monitor developments in the recipient country that could affect your initial assessment. The obligations on the data importer under the SCCs should help here, as it is required to inform the data exporter of a change of law that affects its ability to comply with the SCCs.

Doing nothing is not an option

In a world where personal data move seamlessly across borders and it is almost impossible to live without international data transfers, the EDPB guidance seems impractical. While it is prudent for businesses to regularly review and assess the mechanisms for adequately protecting the rights of individuals when their personal data are transferred across borders, to follow the EDPB guidance to the letter may be unrealistic. Having said that, doing nothing is not an option, and businesses must keep their data transfer mechanisms under review and keep an eye open for further regulatory guidance, including the progress of the draft act updating SCCs published on November 12, 2020.[3]

Takeaways

- Understand the data flows of personal data you control.
- Identify the categories of personal data you process and share.
- Assess the adequacy to protect privacy and human rights of the laws of the countries you transfer to.
- Review the data transfer exemptions and/or mechanisms you have in place from the European Union to elsewhere.
- Implement appropriate due diligence and suitable contractual controls with third parties processing personal data for you.

1 Court of Justice of the European Union, "The Court of Justice invalidates Decision 2016/1250 on the adequacy of theprotection provided by the EU-US Data Protection Shield," news release, July 16, 2020, https://bit.ly/3behchs.
2 "Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data," European Data Protection Board, accessed January 5, 2021, http://bit.ly/2JKkTQC.
3 "Data protection - standard contractual clauses for transferring personal data to non-EU countries (implementing act)," European Commission, November 12, 2020, http://bit.ly/2XFeABj.