Schrems II: Now what? New FAQs from EU data protection supervisors provide guidance on data transfers

Data Protection, Privacy and Security Alert

28 July 2020
By: Carol A. F. Umhoefer | Andrew Serwin

The recent invalidation by the Court of Justice of the European Union (CJEU) of the EU-US Privacy Shield in the so-called *Schrems II* decision has created significant uncertainty for many companies. While the CJEU did not invalidate standard contractual clauses (SCCs, commonly referred to as model clauses), the CJEU also stated that businesses need to verify whether the conditions of transfers made pursuant to standard contractual clauses (including the destination country) offer appropriate safeguards to individuals' personal data in accordance with the GDPR – an "essential equivalency" test.

On July 24, 2020, the group of EU data protection supervisory authorities, the European Data Protection Board (EDPB), issued FAQs regarding the *Schrems II* decision, providing guidance on a number of topics and indicating that more is to come.

The FAQs first confirm that there is no grace period to come into compliance, and organizations relying on Privacy Shield for transfers to the US of personal data that is subject to GDPR must immediately implement an alternative transfer mechanism or cease transfers.

Broadly speaking, alternative transfer mechanisms will include those (i) made pursuant to SCCs or binding corporate rules (BCRs), provided an assessment is conducted; or (ii) made pursuant to GDPR Art. 49 derogations for the transfer of personal data. In addition, transfers made to a jurisdiction (such as Canada) that benefits from a decision of the European Commission finding that the jurisdiction provides adequate protection to personal data are still permissible. Future options may include transferring personal data pursuant to a code of conduct approved by an EU supervisory authority.

The EDPB FAQs make clear that the assessment of the adequacy of SCCs or BCRs requires organizations that have been relying on these mechanisms – or will be henceforward – to determine whether those transfers in fact offer appropriate safeguards to individuals' personal data.

Consequently, organizations will need to analyze data flows that involve transfers of personal data outside the EU, and confirm which transfer mechanism (adequacy, SCCs, BCRs, etc.) they are relying upon. Where SCCs or BCRs are used, organizations must determine the adequacy of those transfers and, where the transfer does not afford adequate safeguards, determine if supplemental measures can be put into place to provide essential equivalency to EU laws. If there is no essential equivalency, an alternative transfer mechanism, such as Art. 49 derogations, will need to be identified. Absent essential equivalency or another valid transfer mechanism, the data exporter must cease transfers and process personal data in the EU.

These approaches are discussed below.

SCCs

SCCs are the workhorse of the data transfer world, and will continue to be so. But surveillance laws – whether US laws or similar laws in other countries – and adequacy generally are of particular concern now. The CJEU held that SCCs may not always sufficiently ensure the effective protection of transferred personal data, in particular "where the law of that third country allows its public authorities to interfere with the rights of the data subjects to which that data relates." In essence, the CJEU has said that where a jurisdiction's laws do not provide essential equivalency, data transfer might not be appropriate, even using an approved data transfer mechanism.

The judgment thus reiterates the importance that organizations assess, prior to any transfer, whether an appropriate level of essentially equivalent protection for Europeans is respected in the destination country, and specifically the presence of "enforceable rights" and "effective legal remedies." The judgment also underscores the relevancy of the GDPR Art. 45(2) criteria for Commission adequacy decisions when exporters are assessing the safeguards applied to their transfers. This assessment should include:

- Consideration of the laws that apply to the importer; for example, in the US, individuals have rights of redress in respect of protected health information (HIPAA) and remedies under CCPA, BIPA and other laws
- The type of data imported; some data may be inherently less at risk
- The categories of data subjects; data regarding persons that e.g., make purchases of athletic gear from a US website are likely less of interest to national security than persons who are using encrypted mobile applications
- Consideration of the business sector in which the importer operates, and the odds of the importer becoming the subject of surveillance
- The identity of the importer; for example, transfers to an importer subject to antitrust investigations in a regulated industry and in which EU data may be implicated would be riskier than transfers to an importer in a non-regulated, competitive industry

It's also important to keep in mind, as the FAQs point out, that the CJEU's ruling is not limited to transfers to the US, and that transfers to other countries that have not received an adequacy decision from the European Commission must also undergo an assessment to determine whether there is essential equivalence in the destination country. If not, supplemental measures must be implemented; the FAQs do not provide examples of such measures, but indicate that the EDPB is working on this issue.

BCRs

The reasoning adopted by the court in *Schrems II* – observing that SCCs do not bind governments and therefore the data exporter (and the relevant supervisory authority) are responsible for assessing whether transfers are made in

circumstances affording adequate protection – appears to apply equally to BCRs, and this has been confirmed by the EDPB and stated by certain EU authorities. Companies making transfers pursuant to BCRs should review and update the assessments they conducted when implementing BCRs to take account of the criteria enounced in *Schrems II*, and particularly in Art. 45(2).

It also bears noting that the authorities are generally supportive of organizations that elect to adopt BCRs, because of the enterprise-wide commitment to data protection that the BCRs require. Regardless, because it typically takes several years to prepare and obtain approval from the relevant authorities for a BCR application, the Rules are a long-term solution, particularly for companies that relied solely on Privacy Shield for transfers to the US.

Art. 49 derogations

Although the EU authorities have long discouraged reliance on derogations to transfer personal data, considering that they should be used only exceptionally, the CJEU and the EDPB consider the derogations to be an option. The principal derogations are explicit consent; performance of a contract to which the individual is a party; and the establishment, exercise or defence of a claim. As these derogations are subject to strict interpretation, and the EDPB stresses that transfers pursuant to contract performance must be occasional, the derogations will necessarily apply only to specific use cases.

Codes of conduct

Schrems II may increase the pressure on trade organizations to obtain approval of industry codes of conduct for transfers. For the moment however, no codes have been approved, and because they are not enforceable against governments, they will be subject to the same critiques as SCC and BCRs, and therefore an assessment of whether the transfer provides adequate safeguards and possibly the adoption of supplemental measures.

Adequacy decisions

Although none of the Commission's adequacy decisions can now be relied upon by US companies acting as data importers, transfers to recipients in Canada, Israel, Japan, Switzerland or any of the eight other jurisdictions that benefit from adequacy decisions are not (for the moment) affected by the judgment. Particularly for multinational groups, adequacy decisions may still provide a measure of protection for a significant volume of data transfers. However, the 12 adequacy decisions that are still valid after *Schrems II* have been under review by the Commission, and *Schrems II* interprets some of the key criteria for the Commission's adequacy evaluation in such a way as could further call into question existing adequacy. Nor is it clear how the *Schrems II* ruling will impact the pending requests for an adequacy decision by South Korea and the UK.

Ceasing transfers and EU storage

Storing and processing data in the EU (or a country with an adequacy decision) may be a solution for some businesses, particularly when EU affiliates of a multinational are conducting autonomous processing activities with no critical business need for the information to be shared with the US parent. The impact of the federal Cloud Act on these issues remains to be seen.

Properly scoping GDPR exposure

Finally, the *Schrems II* decision and the EDPB FAQs underscore the importance of precisely determining when GDPR does and does not apply to a business' processing activities. There has been a trend for US businesses to casually comply with select requirements under GDPR, or member state ePrivacy laws regulating cookies and direct marketing. *Schrems II* has upped the stakes on determining precisely which processing activities fall under the ambit of GDPR or ePrivacy laws, and businesses would be well advised to review whether and to what extent processing activities do in fact trigger application of GDPR.

Learn more about this development by contacting our data privacy team via PrivacyGroup@dlapiper.com.

AUTHORS

Carol A. F. Umhoefer
Partner
Miami | T: +1 305 423 8500
carol.umhoefer@dlapiper.com

Andrew Serwin
Partner
San Diego (Golden Triangle) | T: +1 858 677 1400
andrew.serwin@dlapiper.com