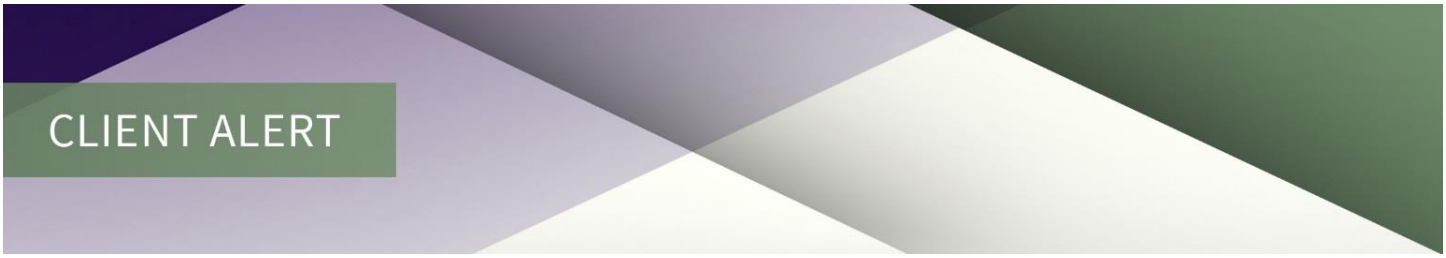

European Data Protection Board Guidance following Schrems II

November 19, 2020

AUTHORS

Daniel K. Alvarez | Richard M. Borden | Henrietta de Salis | Marilena Hyeraci
Dominique Mondoloni | Stefan Ducich

On November 10, 2020, the European Data Protection Board ("EDPB") proposed for public comment guidance on the lawful transfer of personal data from the European Union ("EU") to countries outside the EU – including the U.S. – following the groundbreaking *Schrems II* decision earlier this year. While the Recommendations offer some clarifications and guidance as to steps organizations can take to address compliance concerns, they also underscore a perceived incompatibility between the essential guarantees of data privacy under EU law and U.S. law enforcement/intelligence gathering methods.

The Recommendations highlight the practical difficulties – and technological complexities – associated with protection of privacy in increasingly borderless global commerce and the potential reach of law enforcement agencies. For companies that rely on the transfer of personal data from the EU to, or through, the U.S., or other jurisdictions without an adequacy decision, increased compliance obligations will likely result.

Background

In July 2020, the European Union Court of Justice ("CJEU") invalidated the EU-U.S. Privacy Shield Framework in *Schrems II*, forcing organizations that had been relying on the Framework to identify and execute other mechanisms for legally transferring personal data from the EU to the U.S. Concurrently, *Schrems II* upheld the Standard Contractual Clauses ("SCCs") as a tool to lawfully transfer personal data to a jurisdiction without a European Commission adequacy decision, but the Court's reasoning – with respect to both the Framework and the SCCs – raised numerous practical

questions about what data importers and exporters must do to ensure the protection of personal data at a level essentially equivalent to that guaranteed under EU law.

On November 10, the EDPB proposed, and opened for public comment, Recommendation 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, and Recommendation 02/2020 on the European Essential Guarantees for surveillance measures (the "Recommendations"). The Recommendations are meant, at least in part, to address the questions raised by the *Schrems II* decision, and to detail what the EDPB considers unjustifiable interference by law enforcement in a third country which would render protections of personal data in such jurisdictions inadequate under EU law.

EDPB Recommendations

The Recommendations are based on the premises that data protection is an affirmative and ongoing obligation, the privacy rights of EU citizens remain attached to their personal data regardless of the location of processing, and data exporters and importers are accountable for protecting those rights. According to the EDPB, data exporters and importers must actively analyze and assess whether the relevant transfer tool (e.g., the SCCs) alone is sufficient to provide adequate protection on a case-by-case basis; if not, then identifying and employing appropriate supplemental safeguards are required. And where adequate protection cannot be attained, the Recommendations explain that the data exporter should suspend the transfer of any data and/or terminate the contract with the data importer.

To guide this analysis, Recommendation 01/2020 lays out the following steps:

1. *Know your transfers* – this is primarily an obligation on the data exporter to map where personal data is going to ensure it will receive an essentially equivalent level of protection wherever it is processed;

2. *Identify the transfer tools you are using* – e.g., SCCs or binding corporate rules;

3. *Assess the effectiveness of those tools in light of the circumstances of the transfer* – this requires knowing whether there is anything in the law or practice of the country where the data will be processed that may impinge on the effectiveness of the appropriate safeguards of the transfer tools being used;

4. *Adopt and implement supplementary measures where appropriate* – if necessary to bring the level of data protection up to the EU standard of essential equivalence; and

5. *Reevaluate at appropriate intervals* – compliance is a continuous process, not a one-and-done effort.

This process must be transparent, well documented, and offer effective remedies if the transfer tool is deemed insufficient on its own to ensure adequate protection. For example, in *Schrems II*, the CJEU reasoned that the Privacy Shield Framework was undermined by the lack of minimum safeguards vis-à-vis U.S. surveillance activities (such as those under section 702 of the Foreign Intelligence Surveillance Act), such that the level of protection afforded to data subjects under the Framework was not sufficient under EU law. Applying the rationale more broadly, SCCs or other transfer tools arguably may only be relied on, with respect to transfers to the U.S., if additional supplementary technical measures (such as encryption) provide sufficient safeguards.

In relation to step 3, the data importer – together with the data exporter – will have to assess the applicable laws of the country to which the transfer is to be made. This assessment should take into consideration the rights of redress that the data subjects may have in the case of access to the transferred data by public authorities in that country, as well as the ability of such public authorities to access any personal data (e.g., for criminal law enforcement, regulatory supervision, and national security purposes).

Annex 2 of Recommendation 01/2020 discusses supplemental measures that organizations may employ and provides a non-exhaustive set of use cases. The supplemental measures could include:

(i) Contractual obligations to use specific technical measures or take specific actions;

(ii) Transparency obligations (e.g., providing certain information on local laws);

(iii) Empowering data subjects to exercise their rights; and

(iv) Organizational measures to ensure consistent protection of personal data during all processing activities (e.g., *ad hoc* internal policies, organizational methods in intra-group data transfer).

These measures aim to protect the rights of data subjects by precluding potentially infringing access by public authorities to personal information, whether in transit or in the hands of the data importer.

Annex 2 also identifies certain scenarios where *no* effective supplemental measures could be found. These could significantly impact many companies' operations. For example, the EDPB detailed a scenario where a data exporter uses a cloud provider or other processors situated in third countries without equivalent protections, and which require access to data "in the clear," meaning unencrypted data can be processed in that third country (e.g., the U.S.). The EDPB also discussed a situation where a data exporter makes personal data available to entities in a third country for shared business purposes, such as for personnel services. *In both examples, the Recommendation suggests that there are no effective supplemental measures, and any efforts to protect such data would likely be considered insufficient for GDPR purposes.*

Finally, Recommendation 02/2020 provides more detail on considerations as to whether a country's legal framework governing access to personal data by public authorities, including security agencies, can be regarded as "justifiable interference" (and therefore not impinging on the relevant safeguards of the transfer tool). It clarifies the principles that (i) processing should be based on clear, precise, and accessible rules; (ii) necessity and proportionality with regard to the legitimate objectives pursued need to be demonstrated; (iii) an independent oversight mechanism should exist; and (iv) effective remedies need to be available to individuals.

Practical Outcomes

The proposed Recommendations – and in particular the roadmap and use cases set forth in Recommendation 01/2020 – suggest a level of analysis, both procedural and technical, that will likely involve new and burdensome processes for the many organizations that transfer personal data from the EU to the U.S. and other countries. For instance, prior to initiating the transfer, data exporters must (i) map the flow of data, including onward transfers; (ii) verify whether the data is relevant and limited to what is necessary to fulfill the purpose; and (iii) assess whether the data will be stored in a cloud environment located outside the EU or if it is accessible remotely. The data exporter must then identify the tool it will use, assess its effectiveness under the circumstances, consider whether supplementary technical, contractual and/or organizational measures are necessary and sufficient to establish an adequate level of protection, and if so implement such measures.

These supplemental measures, in particular, go beyond information governance and will require a significant level of analysis and understanding of the technical, administrative, and operational aspects of these data transfers. For instance, the proposed Recommendations suggest that any supplemental technological measures must be state-of-the-art and, among other requirements, encryption must be implemented "flawlessly" and keys managed reliably. This implies deep technological know-how, and will prove burdensome for many organizations, particularly those with anything less than the most sophisticated in-house information security programs. Most importantly, the proposed Recommendations identify certain use cases that, according to the EDPB, cannot be justified regardless of any technical safeguards or supplemental measures.

This position is going to prove extremely problematic for many companies that provide administrative, technical, and other support services to other companies. For example, virtually all Software-as-a-Service providers need access to decrypted data and/or to hold the encryption keys. Likewise, Platform-as-a-Service and Infrastructure-as-a-Service providers typically operate using a shared security model (i.e., encryption keys are held jointly by the controller and processor). As such, implementing the Recommendations as proposed may require significant changes to system architecture. And in some cases, absent pseudonymization, split data, or other methods, it may not be possible to apply supplementary technical measures sufficient to meet the concerns identified by the EDPB.

What's next?

While the proposed Recommendations provide clarity to several of the open questions from *Schrems II*, the EDPB left open – or opened anew – several questions. U.S. and EU companies with trans-Atlantic operations will need to carefully scrutinize each transfer to determine consistency with the identified use cases and applicable technical safeguards.

Meanwhile, the UK is still awaiting a decision from the EU as to whether its data privacy laws are "adequate" such that transfers of data can continue between the EU and the UK following the end of the transitional period on December 31, 2020. If the EU does not grant an adequacy decision, transfers from the EU to the UK will become subject to the processes referred to above in the same way as transfers between the EU and the U.S. The UK Information Commissioner's Office said it is "reviewing the recommendations and will consider whether … to publish [its] own guidance."

Finally, the European Commission has published a new, draft set of SCCs that are intended to account for the complexity of modern processing and changes to data processing activities since the current SCCs were adopted over a decade ago. These updated SCCs are expected to be adopted in early 2021. The draft version employs a modular form and contemplates many more permutations as to data flows than the current SCCs, including transfers from an EU processor to a controller in a third country. Importantly, there will be a transitional period of one year to adopt the new SCCs once they come into effect; however, for any data exporters currently transferring data in accordance with the existing SCCs, the requirement to consider supplementary measures applies immediately upon final adoption of the Recommendations.

The EDPB is accepting feedback on the Recommendations until November 30, 2020.

If you have any questions regarding this client alert, please contact the following attorneys or the Willkie attorney with whom you regularly work.

Daniel K. Alvarez
202 303 1125
dalvarez@willkie.com

Richard M. Borden
212 728 3872
rborden@willkie.com

Henrietta de Salis
+44 20 3580 4710
hdesalis@willkie.com

Marilena Hyeraci
+39 02 76363 1
mhyeraci@delfinowillkie.com

Dominique Mondoloni
+33 1 53 43 45 68
dmondoloni@willkie.com

Stefan Ducich
+1 202 303 1168
sducich@willkie.com