Post-*Schrems II*: European Data Protection Board's Recommendations Bring Further Clarity and Practical Steps Regarding International Data Flows

Skadden

11 / 30 / 20

If you have any questions regarding the matters discussed in this memorandum, please contact the following attorneys or call your regular Skadden contact.

Stuart D. Levi
Partner / New York
212.735.2750
stuart.levi@skadden.com

Eve-Christie Vermynck
Counsel / London
44.20.7519.7097
eve-christie.vermynck@skadden.com

Daniel Millard
Associate / London
44.20.7519.7201
daniel.millard@skadden.com

Oscar XT Tang
Associate / London
44.20.7519.7249
oscar.tang@skadden.com

One Manhattan West
New York, NY 10001
212.735.3000

On November 10, 2020, the European Data Protection Board (EDPB) adopted its long-awaited recommendations on (1) measures that supplement transfer tools to ensure transfers of personal data outside the European Economic Area (EEA) are adequately safeguarded (the supplementary measures recommendation") and (2) the European Essential Guarantees for surveillance measures (the surveillance recommendation). Organizations will now have clearer guidance of the road map to follow when transferring data outside the EEA through the implementation of a detailed multistep plan that covers the diligence of the envisaged transfer and the monitoring of contractual and security safeguards for the transfer over time, among other matters. The supplementary measures recommendation is currently in draft form and remains open to feedback through a public consultation until December 21, 2020, after which the final recommendation will be issued.

Background

Under the General Data Protection Regulation (2016/679) (GDPR), a valid data transfer mechanism must be implemented to transfer personal data out of the EEA to a country that has not been deemed by the European Commission (EC) to have an adequate level of privacy protection.

On July 16, 2020, the Court of Justice of the European Union (CJEU) ruled on two key data transfer mechanisms in *Schrems II*, invalidating the EU-U.S. Privacy Shield for data transfers to the U.S. and imposing enhanced due diligence on parties using the EC Standard Contractual Clauses (SCCs).[1] Under the ruling, where such enhanced due diligence determines, on a case-by-case basis, that the laws of the data importer's country do not provide *essentially equivalent* protection of personal data to that guaranteed under EU law, supplementary measures must be implemented. If the imposition of such supplementary measures would still not provide essentially equivalent protection with respect to the data importer's country, the data transfer must be suspended. The CJEU did not provide further guidance on assessing the laws of third countries, or the form that supplementary measures may take, leaving data exporters uncertain about practical next steps.

As discussed below, the recommendations provide further clarity on these key points through a road map for organizations to follow when transferring data outside the EEA using one of the Article 46 GDPR data transfer mechanisms.

Step 1: Map and Document Your Data Transfers

The recommendations restate the obligation stated in the GDPR that, as a preliminary step, organizations must map, document in writing, and be accountable for their data transfers. This means that on an ongoing basis, organizations should identify (1) what data they transfer outside the EEA; (2) what countries that data is transferred to (including onward transfers); and (3) the mechanism being relied on by the data exporter to transfer the data under the GDPR. The transfer mechanism utilized may be based on an adequacy decision, an Article 46 GPDR mechanism (such as SCCs or binding corporate rules) or an Article 49 derogation (such as where the transfer is necessary for the performance of a contract). Organizations that rely upon Article 49 GDPR derogations to transfer data outside the EEA must ensure that any such transfers are occasional and nonrepetitive, and where such transfers become regular, an alternative transfer mechanism under Article 46 GDPR should be considered.

[1] For further detail on the CJEU's decision, please see Skadden's July 2020 client alert, "*Schrems II*: EU-US Privacy Shield Struck Down, but European Commission Standard Contractual Clauses Survive."

Post-*Schrems II*: European Data Protection Board's Recommendations Bring Further Clarity and Practical Steps Regarding International Data Flows

Step 2: Do Your Diligence

Schrems II imposed the requirement that where organizations, including those located in the U.S., transfer data to a third country pursuant to an Article 46 GDPR data transfer mechanism, they need to consider whether the laws or practices in that third country would undermine the effectiveness of the selected safeguards in relation to EEA data. As described in the supplementary measures recommendation, these safeguards must "travel with the data wherever it goes." The recommendations now affirm that this will entail a thorough and documented due diligence exercise, taking into account both the third country's data privacy framework and its legal landscape more generally.

A key feature of this diligence is an analysis of the access third country public authorities will have to personal data and whether that access is within the limits of what is strictly necessary. To assist with this analysis, in the surveillance recommendation the EDPB has advanced four European Essential Guarantees (EEGs) that the data exporter, with the assistance of the data importer, must assess and identify the presence of before data can be transferred to that third country:

- **Guarantee A: "Processing should be based on clear, precise and accessible rules."** The parties should work cooperatively to identify the laws, regulatory requirements and local surveillance programs in the data importer's country that would govern the interception of individual communications. By undertaking this diligence, the parties should identify, to the extent possible, in what circumstances and on what conditions the data importer's local authorities may request or intercept personal data, whether minimum safeguards are imposed and whether the rules are actionable before a local judicial authority.
- **Guarantee B: "Necessity and proportionality with regard to the legitimate objectives pursued are demonstrated."** Organizations must consider whether the importance of the public interest objective justifies the seriousness of the interference and whether appropriate limitations counterbalance the powers of surveillance of the data importer's local authorities. Data intercepted and stored on a generalized basis will be unlikely to satisfy the requirement of necessity. The recommendations do not provide a clear road map for this analysis and the assessment of Guarantee B may be a difficult exercise for organizations to carry out in practice.
- **Guarantee C: "There should be an independent oversight mechanism."** Organizations should consider the scope of oversight afforded to the courts and regulatory authorities in the data importer's country and the extent of that oversight in practice.
- **Guarantee D: "Effective remedies need to be available to the individual."** In particular, organizations should consider whether EEA data subjects are notified when their data has been collected and whether relevant local bodies or authorities can make binding decisions on the intelligence services.

The EEGs reflect the balancing exercise that the data exporter and data importer must undertake prior to effecting a data transfer to demonstrate that a limitation on data protection and privacy rights is justifiable. However, the surveillance recommendation does not offer parties one clear, straightforward path to reach an answer to this question, and this assessment seems likely to be a challenging portion of the diligence analysis.

Step 3: Safeguard Your Transfers

As previewed in *Schrems II*, where the outcome of the foregoing diligence indicates that an essentially equivalent level of protection as granted in the EEA cannot be guaranteed in a third country, organizations must implement enhanced measures to address both: (1) the likelihood of their data being intercepted while in transfer; and (2) the data importer's obligations in the context of any onward transfers (where authorized) of EEA data. On a case-by-case basis, the supplementary measures recommendation requires organizations to implement appropriate safeguards in the form of contractual and security (technical and organizational) measures to address the identified vulnerabilities in the third country prior to proceeding to the data transfer.

While the supplementary measures recommendation stresses that contractual provisions alone will not suffice, data exporters should nonetheless consider how their current contractual agreements can be enhanced by additional measures. This may include supplementary contractual requirements on the data importer to (1) implement additional technical measures (*e.g.*, encryption), (2) publish regular transparency reports detailing governmental requests to access data (*e.g.*, a table showing the number of data access requests received by the data importer on an annual basis and the percentage of those requests where data is disclosed; where the request is challenged; and where the number of records and/or data subjects disclosed is less than initially requested), (3) monitor legal and/or policy developments and inform the data exporter of any changes that may affect their continued compliance with the data transfer contractual commitments, (4) insert "warrant canaries," in which the data importer is required to send the data exporter cryptographically signed messages at regular intervals confirming it has not received any disclosure requests that would involve EEA personal data, and (5) assist with the handling of EEA data subject rights requests.

Post-*Schrems II*: European Data Protection Board's Recommendations Bring Further Clarity and Practical Steps Regarding International Data Flows

Depending on the outcome of the diligence exercise, the supplementary measures recommendation encourages organizations to implement these measures as soon as reasonably practicable. Contractual provisions can be implemented immediately and, unless they conflict with the SCCs, do not require preapproval from the competent supervisory authority.

Many of these contractual safeguards have been incorporated into the new draft SCCs, published by the EC on November 12, 2020, and currently under public consultation until December 10, 2020 (There will be a one-year grace period applicable to the new set of SCCs). When implementing supplemental contractual protections with the data importer, the data exporter may wish to incorporate or make reference to these new draft SCCs to assist with their drafting.

The supplementary measures recommendation also advises data exporters to consider the following technical and organizational measures:

Supplementary Measures Recommendation	
Technical Measures	– Encryption with algorithms that are "flawlessly implemented" (*e.g.*, by software certified to be specified to that algorithm). – Control over decryption, in transit and at rest, retained by data exporters located in the EEA or a country subject to an adequacy decision. – Pseudonymization, where the data exporter alone retains control over reidentification. – Split or multiparty processing (with sensitivity to any collaboration between public authorities).
Organizational Measures	– Internal policies of the data importer that allocate responsibility amongst employees for data transfers and implement procedures relating to the receipt and escalation of public authority requests for access to personal data. – Training for employees of the data importer to manage public authority requests for access to personal data. – Implementation by the data importer of strict data access controls (on a need-to know-basis) on receipt of data and appropriate internal confidentiality policies.

Careful attention must be paid to the supplementary measures recommendation's conclusion that no technical measures exist that could sufficiently safeguard the data transfer where (1) that data is transferred to processors in third countries who require access to that data "in the clear," or unencrypted, to execute their assigned task (*e.g.*, cloud service providers) or (2) remote access to data is given to data importers in third countries for shared business purposes (*e.g.*, intra-group data transfers). In these instances, organizations should consider whether an Article 49 derogation may apply (such as an instance where a transfer is necessary for the performance of a contract) or suspend such transfers. The exact scope of the supplementary measures recommendation's position on these two transfers is not clear and ideally further clarity will emerge following the consultation period.

Looking Ahead

The recommendations set forth the mandatory approach that organizations in all countries must follow when transferring EEA data to countries that have not received an adequacy decision. Currently, only Andorra, Argentina, Canada, the Faroe Islands, Guernsey, Israel, the Isle of Man, Japan, Jersey, New Zealand, Switzerland and Uruguay have been recognized by the EC as providing adequate protection, and these adequacy decisions are under continued review.

In the absence of an EC adequacy decision in favor of the U.K. post-Brexit, transfers of data from the EEA to the U.K. will require diligence of the U.K.'s data protection legislation and legal landscape more generally. The U.K. government's recent national data strategy, which points to a rejection of legal barriers to data use, and the recent European Court of Justice decision in *Privacy International*,[2] where U.K. surveillance laws for the bulk collection of data were found to exceed the limits of what was strictly necessary and could not therefore be justified within a democratic society, will both be of particular relevance to this diligence.

In the U.S., it is too early to tell whether President-elect Joe Biden's administration will take a different approach to privacy issues, particularly given the inherent tension that the *Schrems II* decision creates between privacy rights and the activities of law enforcement and intelligence agencies.

Key Takeaways

- As set forth in the flow chart below, the recommendations provide a welcome transfer toolkit and step-by-step guidance that organizations both inside and outside the EEA should refer to throughout the life cycle of their data transfers to third countries. Going forward, the positions taken in the recommendations that currently lack sufficient clarity ideally will be

[2] Case C-623/17, 6 October 2020.

refined through the consultation process. Organizations should start reviewing their data maps and transfers, both current and envisaged, and, where appropriate, implement the relevant set of supplementary measures or consider, where no suitable alternatives are available, seeking the competent EEA supervisory authority's authorization and/or, if none of these options is viable, temporarily suspending any transfers which would be deemed uncompliant.

- It also is crucial that organizations now carry out transfer impact assessments (prior to the transfer), regularly monitor their data transfers and document all actions, including diligence, and decisions relating to such transfers. The duty to be "on top of your transfers" will include continued reassessment of the laws of the third countries to which data is transferred and the corresponding adequacy of the adopted data transfer mechanism.