EDPB Adopts Recommendations on Supplementary Measures for Data Transfers Following Schrems II Decision

Article By
Hunton Andrews Kurth’s Privacy and Cybersecurity
Hunton Andrews Kurth
Privacy and Information Security Law Blog-Hunton Andrews Kurth

Related Practices & Jurisdictions
- Communications, Media & Internet
- Administrative & Regulatory
- Global
- All Federal
- European Union

Thursday, November 12, 2020

On November 11, 2020, the European Data Protection Board (the “EDPB”) published its long-awaited recommendations following the Schrems II judgement regarding supplementary measures in the context of international transfer safeguards such as Standard Contractual Clauses (“SCCs”) (the “Recommendations”). In addition, the EDPB published recommendations on the European Essential Guarantees for surveillance measures (the “EEG Recommendations”), which complement the Recommendations. The Recommendations are subject to a public consultation, which closes on November 30, 2020.
As a result of the *Schrems II* judgment, controllers relying on a transfer mechanism under Article 46 of the EU General Data Protection Regulation ("GDPR") to transfer personal data outside the European Economic Area ("EEA") ("data exporters") must verify, on a case-by-case basis and in collaboration with the data importers, as appropriate, whether the law of the importer’s country ensures a level of protection for the personal data that is essentially equivalent to the EEA’s protections. If not, data exporters need to assess whether they can implement supplementary measures to help ensure the requisite level of protection.

The Recommendations are intended to assist data exporters with the challenge of identifying and implementing such supplementary measures. Accordingly, the Recommendations include a 6-step process outlining the steps data exporters must take to determine if they need to identify and implement effective supplementary measures. The Recommendations also include examples of supplementary measures, setting forth some of the conditions they must satisfy in order to be effective. In the Recommendations, the EDPB is cautious that it may not be possible to implement sufficient supplementary measures in every case, in which case, transfers might not be possible.

The Recommendations provide that organizations, when making international data transfers, should:

### Map Data Transfers

Map the data transfers that they carry out, keeping in mind that access from a third country (e.g., storage in the cloud outside the EU) constitutes a transfer, and verify that the data transferred is adequate, relevant and limited to what is necessary in relation to the purposes for which it is transferred. The mapping exercise should include onward transfers made by processors to whom data is disclosed.

### Identify Data Transfer Mechanisms

Verify the transfer mechanism under Chapter V of the GDPR that will be relied upon. No transfer mechanism or further steps are required where there is a valid adequacy decision in force from the European Commission with respect to the recipient country. The Recommendations emphasize that the transfer tools listed under Article 46 of the GDPR, e.g. SCCs and binding corporate rules, should be used where transfers are regular and repetitive, and that the derogations provided by Article 49 of the GDPR should only be used for occasional and non-repetitive transfers and “must be interpreted restrictively.”

### Assess Legal System of Recipient Country

Assess whether the law or practice of the data importer’s country may impinge on the effectiveness of the appropriate safeguards of the transfer tools relied on, in the context of the specific transfer, particularly under legislation that prevents the data importer from complying with its obligations under the relevant transfer tool. The Recommendations provide that this should be particularly carefully considered when legislation or regulations governing access to data by public authorities are “ambiguous or not publicly available.” In addition, any onward transfers also should
be considered.

The Recommendations highlight that recognition of the rule of law in the data importer’s country may be relevant in assessing the effectiveness of redress mechanisms available to individuals with regard to unlawful government access to personal data. Where a comprehensive data protection law or an independent data protection authority exists, this may contribute to ensuring the proportionality of government access. In making an assessment as to whether or not there is likely to be unjustifiable government access to data, organizations should consult the EEG Recommendations.

The Recommendations also state that Section 702 of the U.S. FISA “does not respect the minimum safeguards resulting from the principle of proportionality under EU law and cannot be regarded as limited to what is strictly necessary,” meaning that where data importers or any recipients of onward transfers are subject to Section 702 of FISA, additional supplementary technical measures will be required in addition to a transfer tool under Article 46 of the GDPR.

**Consider Supplementary Measures**

If the legal assessment reveals that the recipient third country’s legislation impinges on the effectiveness of the Article 46 GDPR transfer safeguards relied upon, data exporters must identify and adopt supplementary measures, as they are required to provide a standard of protection for the data that is essentially equivalent to that provided by EU law. The supplementary measures appropriate in each case will depend on a number of factors, including the nature of the data transferred and the possibility that it may be subject to onward transfers. Examples of supplementary measures provided by the Recommendations include:

- Technical measures: such as forms of encryption, with encryption keys kept beyond the reach of relevant public authorities, and pseudonymization that does not permit re-identification of data.

- Additional contractual measures: such as obligations to implement the technical measures discussed above, transparency obligations regarding the level of access available to government authorities in the recipient jurisdiction and the measures taken to prevent access to personal data, and reinforced power for the data exporter to conduct audits of the data importer. Data exporters should also consider contractually requiring data importers to review the legality of any access requests received and to challenge such requests where appropriate.

- Organizational measures: such as adoption of internal policies with clear allocation of responsibilities for data transfers and operating procedures in the event of an access request, transparency and accountability measures including documentation of access requests, and ensuring data minimization.

The Recommendations also provide examples of where supplementary measures cannot ensure an appropriate level of protection, such as where the power granted to public authorities of the recipient country to access the transferred data goes beyond what is necessary and proportionate in a democratic society. In these
circumstances, organizations are required to avoid, suspend or terminate the relevant transfer, and data already transferred should be returned or destroyed by the data importer.

**Address Formalities**

Take any formal procedural steps that the adoption of supplementary measures may require, such as seeking authorization from the competent supervisory authority if there is an intention to modify the SCCs.

**Keep Data Transfer Arrangements Under Review**

Re-evaluate at appropriate intervals the level of protection provided and monitor any developments that may affect it. The Recommendations highlight that the principle of accountability requires “continuous vigilance” as to the level of protection of personal data.

In addition, the EDPB adopted the EEG Recommendations to provide data exporters with criteria to assist in determining whether the legal framework of a recipient country, governing public authorities’ access to personal data for surveillance purposes, can be regarded as permitting justifiable interference with the rights of EU individuals to privacy and the protection of their personal data.

The EEG Guarantees provide that, “the applicable legal requirements to make the limitations to the data protection and privacy rights recognized by the Charter [of Fundamental Rights of the EU] justifiable can be summarized in four European Essential Guarantees:

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

The EDPB provides that these “core elements” are not to be assessed independently, but instead holistically, reviewing the relevant legislation having regard to surveillance measures, the minimum level of safeguards for the protection of the rights of individuals, and the remedies provided under the national law of the recipient jurisdiction.

The Recommendations are open for public consultation until November 30, 2020, and feedback may be submitted [here](#). The Recommendations are immediately applicable following their publication.

Copyright © 2022, Hunton Andrews Kurth LLP. All Rights Reserved.

National Law Review, Volume X, Number 317