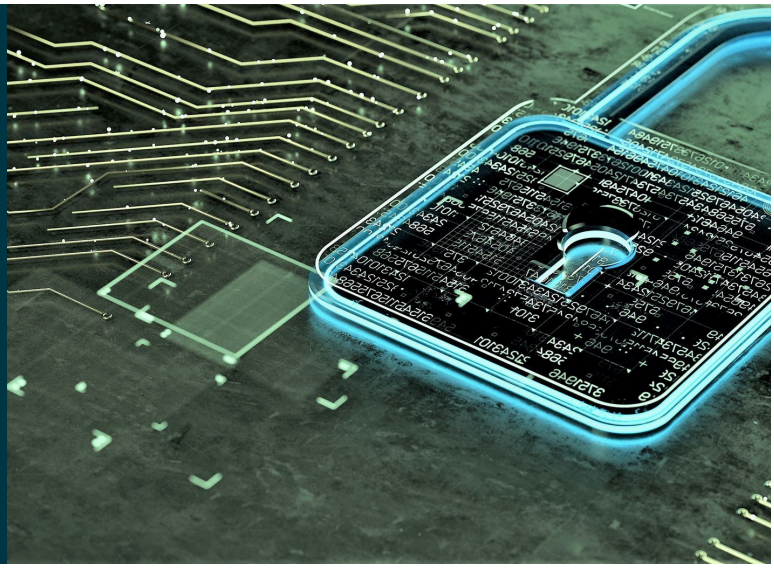
WILSON SONSINI

EDPB Publishes Draft Recommendations on Supplementary Measures for Data Transfers



CONTRIBUTORS


Cédric Burton


Christopher Kuner


Christopher N. Olsen

ALERTS

November 12, 2020

On November 11, 2020, the European Data Protection Board (EDPB), comprised of the European data protection regulators (DPAs), issued two long-awaited sets of recommendations. These recommendations are critical for any companies exporting or importing EU personal data.

The first set contains a roadmap of the steps data exporters should take when relying on EU-approved data transfer mechanisms to transfer data from the European Economic Area (EEA) to another country (**Transfer Tool Recommendations**). The second set of recommendations provides guidance on how to assess a third country's surveillance measures when exporting personal data outside of the EEA (European Essential Guarantees **(EEG) Recommendations**). The latter are relevant to businesses when assessing a third country's level of data protection, and to DPAs when assessing a third country's adequacy. The recommendations are applicable immediately, but the Transfer Tool Recommendations are open for public consultation until November 30. Organizations can provide comments here.

One day later, on November 12, 2020, the EU Commission issued a new set of standard contractual clauses (SCCs) which is now subject to public consultation. This is one of the most significant developments in EU data protection law since the entry into force of the General Data Protection Regulation (GDPR). We will provide further insight on this topic in a subsequent alert.

For a deeper dive on this topic, please register here for our EU privacy and cybersecurity team's webinar on Thursday, November 19, 2020 at 9 a.m. PT / 12 p.m. ET / 6 p.m. CET.

Background

On July 16, 2020, the European Court of Justice (ECJ) invalidated the EU-U.S. Privacy Shield framework and required organizations relying on the SCCs to assess whether the law of the third country to which EEA data is being transferred ensured a level of protection essentially equivalent to the level guaranteed in the EEA (for more background on Schrems II, see our post on The Wilson Sonsini Data Advisor, *ECJ Invalidates EU-U.S. Privacy Shield and Upholds the Standard Contractual Clauses*). If the safeguards contained in the SCCs are insufficient, organizations exporting data must add supplementary measures to ensure such a level of protection.

A Roadmap to Assess Data Transfers and Implement Appropriate Safeguards

The Transfer Tool Recommendations provide a six-step roadmap to assist organizations exporting data out of the EEA. The roadmap applies to organizations relying on a data transfer mechanism under Article 46 GDPR (in particular, EU-approved standard contractual clauses and Binding

Corporate Rules (BCRs)) to i) determine whether they must supplement data transfer mechanisms with safeguards, and ii) help them identify and implement such safeguards.

1. **Identify and assess the relevant data for data transfers.** Organizations exporting data should limit the transfer to only that which is necessary for its purposes, and prior to the transfer undertake a data mapping exercise to record all data transfers and destinations, including onward transfers. This exercise should also reflect any remote access from a third country or storage by a cloud service provider situated outside of the EEA, unless the provider has contractually provided that data would not be processed in third countries.
2. **Identify the relevant data export mechanism or tool.** If an organization transfers data on the basis of an adequacy decision, it should monitor the validity of the adequacy decision and does not need to take other actions as long as the adequacy decision remains valid. For any other regular and repetitive data transfers, organizations should rely on one of the mechanisms set out in Article 46 GDPR, such as the SCCs or BCRs. The EDPB acknowledges that the GDPR also contains further derogations but that those should be interpreted restrictively and should be used in exceptional circumstances,[1] i.e., only for occasional and non-repetitive transfers.
3. **Assess the data protection laws and practice in the third country.** Organizations should assess the laws and practices of the recipient third country to determine whether they may impinge on the effectiveness of the safeguards of the data transfer mechanism organizations use. The EDPB recommends that organizations first assess the legislation publicly available in the third country, and if such information is not available, assess other relevant factors such as case law and academic reports. Organizations may work with the data importer to obtain such information. Organizations should not rely on subjective factors, such as publicly expressed policy views or enforcement probability. This assessment should be conducted with proper due diligence and documented thoroughly.

   An organization should only transfer personal data if its assessment of a third country's laws and practices indicate that it can offer an adequate level of protection. The EEG Recommendations (discussed below) set out the key elements for organizations to determine whether interference by public authorities in third countries can constitute a justifiable interference to the EU fundamental right to data protection. If an adequate level of protection cannot be achieved, data should not be transferred unless effective supplementary measures are implemented (see step 4 below). The EDPB specifically notes that data transfers subject to section 702 of the U.S. Foreign Intelligence Surveillance Act (FISA) must be supplemented by technical measures to prevent access to the transferred data.
4. **Identify and adopt appropriate supplementary safeguards.** What will constitute appropriate safeguards depends on the specific use of the data. Factors to consider include: the format and nature of the data transferred, the complexity of the data processing workflow, and the likelihood of onward transfers. The EDPB identifies the following potential safeguards as examples:
   1. Technical measures, such as encryption, pseudonymization, and split or multi-party processing (whereby processing will be carried out on multiple separate locations or by multiple parties). The EDPB has not yet identified appropriate technical safeguards for certain scenarios involving unencrypted data processing, or when the data importer is in possession of the cryptographic keys to decrypt data for the provision of its services.
   2. Contractual requirements, such as i) commitments to use specific technical measures, ii) the publication of transparency reports and other information on access by public authorities, iii) obtaining certifications and conducting audits, iv) taking specific actions (such as notifying the data exporter if the data importer cannot comply with its obligations), v) a prohibition against engaging in onward transfers, or vi) assisting data subjects in exercising their rights.
   3. Organizational measures, such as the adoption of internal policies, developing best practices and disciplinary measures and documenting data access requests.

   If an organization cannot implement effective supplementary measures, it must cease any existing data transfers. If organizations continue to transfer data, the EDPB requires organizations to notify the competent DPA, who may suspend or prohibit such data transfers and impose corrective measures such as fines.
5. **Take steps to implement the supplementary measures.** The necessary steps may vary depending on the data transfer mechanism used. If SCCs are used, organizations are not required to obtain authorization from the competent DPA to implement the supplementary measures listed above as long as such measures i) do not modify the SCCs themselves, ii) do not contradict the SCCs, and iii) sufficiently ensure the required level of protection. The EDPB notes that the impact of Schrems II on BCRs and *ad hoc* contractual clauses is still under discussion and it will provide more details in due course.
6. **Periodically reevaluate safeguards.** Organizations should monitor developments in the third country to assess whether their decisions are still appropriate, and promptly suspend or end data

transfers where the supplementary measures are no longer effective in the third country, or where the data importer is in breach or otherwise unable to fulfill its obligations.

Assessing a Third Country's Legal Framework for Surveillance

The EEG Recommendations complement the Transfer Tool Recommendations and provide organizations with guidance on how to assess whether a third-country's surveillance laws constitute a justifiable interference with the EU data protection rights. This is relevant when assessing the data protection laws and practices of third countries under the third element of the roadmap discussed above.

The EEG Recommendations set out four European Essential Guarantees which need to be addressed by the laws in countries to which data is transferred in order to ensure that government surveillance and access to personal data constitute a justifiable interference to the data protection rights of EU citizens:

1. **Processing should be based on clear, precise, and accessible rules.** A third country's law should be clear, precise, uniformly applied, and foreseeable.
2. **Interferences should be proportionate and necessary with regard to the legitimate objectives pursued.** The limitation of data protection rights must be assessed and balanced against the importance of the public interest objective pursued by the third country. Under certain set conditions the requirement to safeguard national security can justify serious interference with fundamental rights. The laws of the third country should respect the principle of necessity; laws permitting generalized access to the content of electronic communications without objective criteria generally will not meet such requirement.
3. **Independent oversight.** Any interference to data protection rights should be subject to an effective, independent, and impartial oversight mechanism. The EDPB recommends assessing the independence of a court or administrative body by reference to whether their members are political appointees, or whether its activities are open to public scrutiny.
4. **Effective remedies need to be available to the individual.** Individuals must have recourse to obtain sufficient redress and effective remedies to challenge the legality of such surveillance.

Conclusions and Next Steps

These recommendations have a significant impact on any company importing or exporting EU personal data. While the recommendations are not binding, they represent the views of DPAs, which are responsible for enforcing the GDPR. The Transfer Tool Recommendations are subject to public consultation and any impacted party should consider submitting a comment.

In light of these recommendations, companies should carefully assess their data transfers by conducting data transfer impact assessments following the steps outlined by the EDPB. These new assessments represent an additional administrative burden imposed on companies in light of the accountability principle, but they will undoubtedly be requested by regulators pursuant to a complaint or investigation. It is likely that NGOs will file complaints with DPAs or initiate actions before courts against companies transferring personal data in violation of these recommendations.

Our EU privacy and cybersecurity team is closely monitoring this topic, including further guidance from the EDPB on BCRs and ad-hoc contractual clauses, and will provide updates when they are released.

Wilson Sonsini helps companies address complex privacy issues in Europe and other business markets. For more information, please contact Cédric Burton, Laura De Boel, Nikolaos Theodorakis, Chris Olsen, or another member of the firm's privacy and cybersecurity practice.

---

[1] Article 49 GDPR.