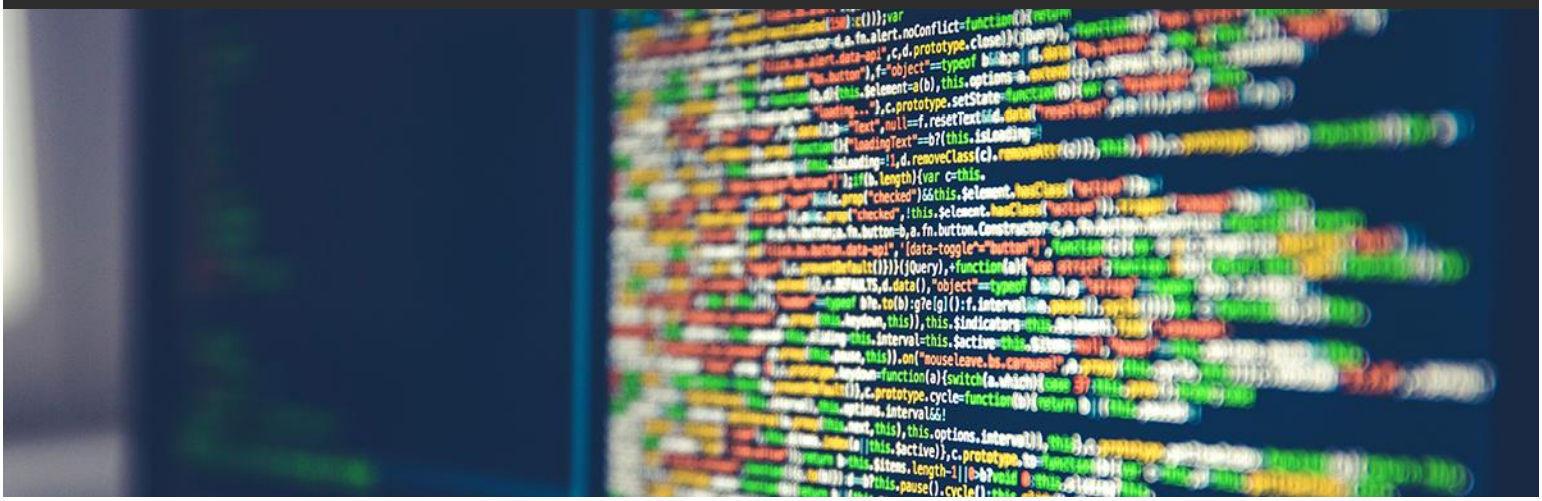
GT GreenbergTraurig

Alert | Data, Privacy & Cybersecurity



November 2020

EDPB Guidance on Supplementary Transfer Measures and Surveillance Calls Into Question Future Use of SCCs for Data Transfers to US

** Please note, post publication the EDPB extended the deadline for public comments on the Supplementary Transfer Measures Recommendations to Dec 21, 2020.*

On Nov. 11, the European Data Protection Board (EDPB) published Supplementary Transfer Measures Recommendations and Surveillance Recommendations.

Schrems II Judgment & SCCs

This follows the July 2020 *Schrems II* judgment (C-311/18), where the Court of Justice of the European Union (CJEU) invalidated the EU-U.S. Privacy Shield Framework as a legal personal data transfer mechanism to the U.S. because neither U.S. law nor the Privacy Shield provides EU data subjects effective remedies against the far-reaching rights of U.S. intelligence services. In the *Schrems II* judgment, the CJEU also found that under certain circumstances organizations could still rely on Standard Contractual Clauses (SCCs) to transfer personal data from the European Economic Area (EEA) to the U.S. or any other country that the EU considers not to provide an adequate level of data protection (third country) under Chapter V of the General Data Protection Regulation (GDPR). The CJEU explained that, to rely on SCCs for such transfers, the exporting organizations must undertake a case-by-case assessment of the transfer to ensure an essentially equivalent level of protection for the EEA personal data under the third country's

laws, and that in certain circumstances "supplementary measures" may be necessary to ensure such protection. Shortly after the *Schrems II* judgment, the EDPB issued FAQs regarding the *Schrems II* decision, and noted that it would provide more guidance on the "supplementary measures" an exporting organization could consider taking to ensure an adequate level of data protection when using SCCs in relation to such transfers.

Supplementary Transfer Measures Recommendations

In the Supplementary Transfer Measure Recommendations (Transfer Recommendations), the EDPB begins by noting that "transferring personal data to third countries cannot be a means to undermine or water down the protection it is afforded in the EEA," and then goes on for 38 pages to provide data exporters with steps and examples of supplementary measures (Annex 2) that they may consider taking to ensure personal data transferred to a third country is processed in compliance with GDPR principles. The EDPB directs exporting companies to take the following steps to ensure they satisfy Article 5.2's accountability principle, which requires controllers to be responsible for, and be able to demonstrate compliance with, the GDPR principles relating to processing of personal data:

(1) Map all instances where data is being transferred to third countries (including "remote access by an entity from a third country to data located in the EEA"), and ensure the data transferred is in line with the principles of data minimization.

(2) Identify the Chapter V GDPR transfer tool being used for each transfer, such as SCCs, binding corporate rules or Article 49 derogations, which the CJEU describes as having an "exceptional nature" and being appropriate "only in some cases of occasional and non-repetitive transfers."

(3) Assess whether the law or practice of the third country prevents the personal data transferred from being afforded an essentially equivalent level of protection as under the GDPR (see Surveillance Recommendations, below).

(4) If the third country's laws or practices do not provide an essentially equivalent level of protection as under the GDPR, identify and adopt supplementary measures that will ensure such protection, to the extent possible.

(5) Take the necessary procedural steps for the implementation of the supplementary measures – which may require consultation with the supervisory authorities.

(6) Regularly reevaluate whether the protection afforded to the personal data transferred has changed due to new laws or practices in the third country.

The EDPB notes that the analysis described above, particularly the assessment of supplementary measures, should be documented.

In Annex 2 of the Transfer Recommendations, the EDPB offers numerous examples of technical, contractual, and organizational supplementary measures and provides scenarios where effective measures exist, and where no effective measures exist such that the transfer would not be valid under Chapter V GDPR. The proposed measures are similar to those previously suggested by the German Federal Commissioner for Data Protection and Freedom of Information (BfDI) in August.

- Effective Supplementary Measures. The EDPB provides five examples of effective supplementary measures, that will work even in a third country where the public authorities' access goes beyond what

is necessary and proportionate in a democratic society. These scenarios include the following scenarios:

- *No Access*. Where the organization in the third country is used for data storage, backup, and other purposes where access to the data is not required if the data is processed using strong encryption that protects against public authorities' cryptanalysis, and encryption keys are retained by the data exporter.
- *Pseudonymization*. Where only pseudonymized data for analysis or research purposes, and only the data exporter holds the additional information to identify the data subject.
- *Data in Transit*. Where encrypted data is routed via a third country to reach an organization located in a country providing adequate data protection if transport encryption is used and decryption is only possible outside the third country, protective measures are used against active and passive attacks, and the encryption algorithm against public authorities' cryptanalysis, no backdoors exist, and encryption keys are managed by the exporter and the entity in the adequate jurisdiction receiving the data.
- *Protected Recipient*. Where personal data transferred to an importer in a third country is specifically protected by that country's laws, such as for medical treatment or legal services, and the data is encrypted prior to transmission, the data importer does not share the data with a processor in a way that permits public authorities to access the data, the decryption key is in the sole custody of the data importer.
- *Split of Multi-Party Processing* Where the data exporter wants two or more independent processors located in different jurisdictions to process the data, and splits the data such that neither processor can identify a specific data subject with the data they are provided, or the data is processed jointly in such a way that no information is revealed to either that they did not possess prior to the join processing.

- Ineffective Supplementary Measures. The EDPB notes that, even where transit and at Rest encryption are in place, the following types of transfers to a third country not providing an adequate level of data protection would not be compliant with the GDPR; (1) transfer of data to cloud service providers or other processors requiring access to data; and (2) where a related company in a third country accesses data for business purposes, uses the data in the clear for its own purposes, and public authorities' access to such data goes beyond what is necessary and proportionate in a democratic society.

In those scenarios where supplementary measures can be taken, specific contract provisions will likely need to be adopted, such as provisions that require an importer to:

- identify the specific technical measures,
- identify the steps taken to prevent access by public authorities in compliance with the European Essential Guarantees for surveillance measures,
- agree to inform the exporter every 24 hours that it has not received an order to disclose personal data,
- guarantee not to create backdoors in its system to access data,
- provide the exporter with increased audit rights,
- notify a data subject of any third-party requests for their information prior to disclosure,
- guarantee that access only be granted upon data subject's consent,
- assist the data subject in exercising their rights in the third country, and

- commit not to engage in any onward transfer of the personal data when a level of protection equivalent to the EU cannot be guaranteed.

Some of the other supplementary measures noted include:

- regular publication of transparency reports regarding governmental requests,
- adoption of strict and granular access and confidentiality policies,
- adoption of best practices based on a strict need-to-know principle,
- regular audits, and
- adoption of strict data security and data privacy policies based on EU certification codes of conducts and international standards.

Surveillance Recommendations

The EDPB's Surveillance Recommendations are provided to further develop the European Essential Guarantees (EEGs), drafted by the Article 29 Working Party in response to the *Schrems I* judgment, in light of the *Schrems II* judgment and to provide further guidance on assessing whether an importing country's surveillance measures which allow access to personal data by national security agencies or law enforcement authorities can be considered a justifiable interference or invalidate the transfer.

The Surveillance Recommendations analyze this issue in relation to the four EEGs:

(1) processing should be based on clear, precise, and accessible rules;

(2) necessity and proportionality with regard to the legitimate objectives pursued must be demonstrated;

(3) an independent oversight mechanism should exist; and

(4) effective remedies need to be available to the individual.

The Recommendations note that the EEGs "require a certain degree of interpretation, especially since the third country legislation does not have to be identical to the EU legal framework," and depend on "all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorize, carry out and supervise them, and the kind of remedy provided by national law."

EDPS Strategy for EUI Transfers

On Oct. 30 the European Date Protection Supervisor (EDPS) issued a Strategy for Union institutions, offices, bodies, and agencies [EUIs] to comply with the *Schrems II* ruling (EDPS Strategy), with the goal of ensuring ongoing and future international transfers comply with the EU Charter of Fundamental Rights and the GDPR. The EDPS strongly encourages EUIs to avoid processing activities that involve transfers of personal data to the United States.

EUIs will be required to complete a case-by-case Transfer Impact Assessments (TIAs) to identify whether an essentially equivalent level of protection exists under the importing country's law for each transfer. Following the finalization of EDPB's guidance on supplementary transfer measures, it will provide a list of

preliminary questions for EUIs to use in the TIAs. Thereafter, the EDPS plans to establish long-term compliance priorities.

Authors

This GT Alert was prepared by:

- Gretchen A. Ramos | +1 415.655.1319 | ramosg@gtlaw.com
- Carsten Kociok | +49 30.700.171.119 | carsten.kociok@gtlaw.com
- Darren Abernethy | +1 415.655.1261 | abernethyd@gtlaw.com