Bond

INFORMATION MEMO
CYBERSECURITY AND DATA PRIVACY

JULY 29, 2020

EDPB Issues Guidance on Data Transfers After CJEU's Decision Invalidating the EU-U.S. Privacy Shield

The decision of the Court of Justice of the European Union (CJEU), in *Schrems II*, invalidating the EU-U.S. Privacy Shield has engendered significant uncertainty regarding data transfers from the EU to the United States. In reaction, the European Data Protection Board (EDPB), an association of representatives of the EU data protection authorities (DPAs), has issued guidance on *Schrems II* in the form of answers to twelve frequently asked questions received by DPAs relating to the decision.

First, the EDPB's guidance clarifies that there is no stated grace period for the *Schrems II* decision to take effect. Therefore, if your organization is solely relying on the EU-U.S. Privacy Shield to transfer data outside of the European Economic Area (EEA), those transfers are now illegal and may only continue if your organization implements another established transfer mechanism pursuant to the EU's General Data Protection Regulation (GDPR).

Second, the use of Standard Contractual Clauses (SCCs) and Binding Corporate Rules (BCRs) pursuant to Article 46 of the GDPR remains an option, but only if the country of destination provides an adequate level of protection or if certain supplementary measures are put in place to ensure an essentially equivalent level of protection as provided by the EEA.

Regarding data transfers to the United States pursuant to SCCs or BCRs, the EDPB noted that the CJEU held that U.S. law does not ensure an essentially equivalent level of protection. The EDPB, like the CJEU, specifically pointed to Section 702 of the Foreign Intelligence Surveillance Act and Executive Order No. 12,333 as the basis for the determination that U.S. law failed to ensure an adequate level of data protection. According to the guidance, continued transfers to the U.S. pursuant to SCCs or BCRs require an assessment of whether supplementary measures are sufficient to ensure a level of protection equivalent to that guaranteed within the EEA. Unfortunately, the EDPB did not provide any guidance on what supplementary measures might be sufficient to ensure that the SCCs or BCRs provide an adequate level of protection. The EDPB stated that it was analyzing the issue and intends to issue further guidance.

Third, the EDPB stated that it is currently assessing the impact of the *Schrems II* decision on the other transfer mechanisms permitted under Article 46 of the GDPR. The EDPB provided no additional guidance, but noted that the standard for appropriate safeguards under any of the mechanisms permitted under Article 46 is essential equivalence to the protections afforded within the EEA.

Fourth, the guidance states that it is still possible under certain circumstances to transfer data from the EEA to the U.S. pursuant to the derogations set forth in Article 49 of the GDPR. For transfers based on the consent of the data subject pursuant to Article 49(1)(a), the consent must be: (i) explicit, (ii) specific for the particular data transfer and (iii) informed. With respect to the final requirement—that the consent be "informed"—the EDPB noted that the data subject should be informed of the specific risks resulting from the fact that their data will be transferred to a country that does not provide adequate protection and that no safeguards aimed at ensuring adequate protection are implemented.

For transfers necessary for the performance of a contract between the data subject and the controller pursuant to Article 49(1)(b), the EDPB noted that personal data may only be transferred when the transfer is "occasional" and objectively necessary for the performance of the contract.

For transfers necessary for important reasons of public interest pursuant to Article 49(1)(d), the EDPB emphasized that the essential requirement for the applicability of this derogation is the nature of the public interest, not the nature of the organization. The guidance also notes that while this derogation is not limited to occasional use, it is not permissible to use this derogation to implement data transfers on a large scale in a systematic manner.

Finally, the EDPB addressed whether it is permissible to continue to use the services of a processor if the contract, signed in accordance with Article 28.3 of the GDPR, indicates that data may be transferred to the U.S. or another country that lacks adequate protection. The guidance states that if none of the transfer options can be implemented in a manner ensuring essentially equivalent data protection as afforded in the EEA, the only solution is to alter the contract to forbid transfers to the U.S. or the third country. Under such circumstances, the EDPB emphasized that data should not be stored or administered in the U.S. or the third country.

We will continue to update you regarding the legal ramifications and impact of the *Schrems II* decision on data protection. For more information on how to navigate the everchanging landscape of data privacy and international data transfers, please contact Jessica Copeland, John Clopper or any of the attorneys in the Cybersecurity and Data Privacy practice.