Bond

INFORMATION MEMO
CYBERSECURITY AND DATA PRIVACY

JULY 16, 2020

High Court in the EU Strikes Down Privacy Shield

After years of United States organizations—large and small—investing in and relying on the EU-U.S. Privacy Shield as the foundation for permissible data transfer between the EU and the U.S., with the stroke of a pen, or strike of a keyboard, the highest court in the EU invalidated the Privacy Shield.

By way of background, under the General Data Protection Regulation (GDPR), transfer of data outside of the European Economic Area (EEA) may only take place if the receiving country ensures an adequate level of data protection. The European Commission, pursuant to Article 45 of the GDPR, has designated certain non-EU countries as countries that provide an adequate level of data protection (Adequacy Decision).[1] If an Adequacy Decision is made relating to a specific country, data may be transferred outside of the EEA to that country without the requirement of any transfer mechanism. An Adequacy Decision was initially made for the United States, but only if such data transfer was limited to the Privacy Shield framework. Prior to the decision in *Data Protection Commission v. Facebook Ireland and Maximillian Schrems*, Case C-311/18 (Schrems II), there were four ways in which an organization outside of the EEA would be deemed "adequate" to permit data transfer to the United States: (1) certification under the EU-U.S. Privacy Shield; (2) use of EU Standard Contract Clauses (SCCs); (3) adoption of Binding Corporate Rules (BCRs);[2] or (4) through derogations, including with data subject consent or for the performance of a contract (collectively known as Data Transfer Mechanisms).

In *Schrems II*, Maximillian Schrems, an Austrian national residing in Austria, and Facebook user since 2008,[3] filed a complaint with the Irish Supervisory Authority seeking to prohibit the transfer of his personal data from Facebook Ireland to Facebook Inc. servers located in the United States. Among other things, Schrems claimed that U.S. laws are insufficient in that they do not prevent or prohibit government access to personal data. The high court held that because the United States does not adequately limit government access or surveillance of personal information, its laws alone are inadequate for data protection set forth under the GDPR and therefore invalidated the EU-U.S. Privacy Shield. This eliminates one of the most widely used Data Transfer Mechanisms once accepted by the EU for U.S. organizations to receive EU-resident data for the purposes of international commerce. Fortunately, the court did not invalidate the use of SCCs or BPRs, but it did caution that each SCC, and perhaps the capability to fully implement and the actual implementation of the same, could be challenged and evaluated by EU regulators on a case-by-case basis.

Schrems II could significantly impact the free-flow of data internationally. The U.S. Secretary of Commerce, Wilbur Ross, issued the following statement relating to the *Schrems II* decision:

> "While the Department of Commerce is deeply disappointed that the court appears to have invalidated the European Commission's adequacy decision underlying the EU-U.S. Privacy Shield, we are still studying the decision to fully understand its practical impacts,…We have been and will remain in close contact with the European Commission and European Data Protection Board on this matter and hope to be able to limit the negative consequences to the $7.1 trillion transatlantic economic relationship that is so vital to our respective citizens, companies, and governments. Data flows are essential not just to tech companies—but to businesses of all sizes in every sector. As our economies continue their post-COVID-19 recovery, it is critical

1 Currently the list includes: Andorra, Argentina, Canada (commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, and Uruguay.

2 An entity that is international can enter into BCRs, which need to be approved by a Supervisory Authority in the EU. These "rules" are essentially data protection policies adhered to by companies established in the EU for transfers of personal data outside of the EEA. Such rules must be enforced for the entire entity and shall include all general data protection principles and enforceable rights to ensure appropriate safeguards for data transfers. These rules must be legally binding.

3 Facebook Ireland collects data of EU resident Facebook users and transfers it to Facebook Inc. servers located in the United States.

> that companies—including the 5,300+ current Privacy Shield participants—be able to transfer data without interruption, consistent with the strong protections offered by Privacy Shield."[4]

The extensive ramifications of the court's decision are still uncertain at this time. Many large U.S. organizations, including Facebook, Google, Amazon and various cloud-based technology giants have relied on the EU-U.S. Privacy Shield as the mechanism for transferring data across the pond, and many may now be left scrambling to firm up and execute an alternative authorized Data Transfer Mechanism. Additionally, for those relying on SCCs, it is unclear when and how such SCCs may be questioned by the appropriate authorities but one thing is clear, those provisions should be reviewed with your legal team today, and evaluated for internal compliance as well as adequate protections with respect to government access and surveillance.

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, Amber Lawyer, John Clopper, Fred Price or any of the attorneys in the Cybersecurity and Data Privacy practice.

4 It is important to note that the Department of Commerce will continue to administer the Privacy Shield program and enforce certification obligations on participating U.S. entities.