PUBLICATION

The Uncertain Future of Cross-Border Data Transfer Mechanisms

September 14, 2018

Many organizations that transfer data from the European Economic Area (EEA), including the European Union (EU), or Switzerland (which operates as a sovereign nation independent of the EU and EEA) to the United States of America (U.S.) are unaware that several of the cross-border data transfer mechanisms widely in use for EU General Data Protection Regulation (GDPR) compliance are under attack. Standard contractual clauses and the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks are currently used, and were first created, with the intention of meeting the GDPR's requirement that the privacy of cross-border data be "adequately protected", but the continued validity of these mechanisms is uncertain. This uncertainty was most clearly articulated by European regulators when they threatened to suspend these mechanisms by September 1, 2018.

As of the date of this alert, the proposed deadline of September 1 has passed without further action taken by the EU or U.S. Although the EU-U.S. Privacy Shield program has not been suspended, the validity of the program remains threatened and all organizations who transfer data back to the U.S. should continue to analyze their approach.

The CLOUD Act

The mounting skepticism of EU regulators can be traced to numerous events, including the U.S. government's recent passage of the Clarifying Lawful Overseas Use of Data Act (CLOUD Act) which has done nothing to ease the EU's privacy concerns. The CLOUD Act allows U.S. law enforcement (and foreign law enforcement under certain conditions) to compel disclosure of requested data that is stored outside the U.S. from organizations acting as providers of electronic communications services and remote computing services. Unsurprisingly, EU regulators have voiced concerns that the CLOUD Act may conflict with EU data protection laws, particularly with respect to the expansive surveillance activities possible under the CLOUD Act and the recently implemented EU General Data Protection Regulation (GDPR), and its enactment, among other U.S. privacy-related developments being criticized by the EU, may elicit more protective behavior from the EU in the near future.

Indeed, the CLOUD Act has given rise to serious concerns among U.S. organizations as well, prompting them to take a closer look at the nature of their customer service offerings. A recent cautionary tale in that regard came in the form of a U.S. district court decision that expansively interpreted the CLOUD Act as applying to user-to-user messaging services provided by Airbnb. To the surprise of the popular short-term rental platform, the court classified it as a "remote computing service" provider subject to the CLOUD Act.

EU-U.S. Privacy Shield

The EU-U.S. Privacy Shield Framework allows organizations to self-certify to the U.S. Department of Commerce and publicly commit to comply with the Framework's requirements, including certain data protection measures for transferring personal data from the EU or EEA to the U.S. Although joining the Privacy Shield program is voluntary, once an organization publicly commits to comply with the program's requirements, its commitment is enforceable by the Federal Trade Commission under U.S. law.

On June 11, 2018, the European Parliament's Civil Liberties Committee passed a resolution to suspend the EU-U.S. Privacy Shield program if the U.S. does not demonstrate its compliance with the program by the

September 1 deadline. The resolution is non-binding, so the European Commission, which has the final decision on this, could choose to ignore the proposed deadline. Nevertheless, the resolution reflects the view shared by many European regulators that the Privacy Shield program fails to adequately protect the personal data of Europeans. This lack of confidence in the U.S.-administered program is rooted in reductions in individual privacy rights perceived by the EU in recent U.S. legal, legislative, and executive developments, as well as discomfort resulting from highly publicized privacy scandals, such as the data harvesting incident involving U.S.-based social media platform Facebook and consulting firm Cambridge Analytica.

On October 18 and 19, EU and U.S. regulators will hold their second annual review of the EU-U.S. Privacy Shield Framework. Although the Privacy Shield passed its first annual review in 2017, its passage this year seems more precarious in light of the many unresolved concerns about it held by EU regulators.

Swiss-U.S. Privacy Shield

Similar to the EU-U.S. Privacy Shield Framework, the Swiss-U.S. Privacy Shield Framework allows organizations to self-certify to the U.S. Department of Commerce and publicly commit to comply with the Framework's requirements when transferring personal data from Switzerland to the U.S. Although there has been less news coverage about what concerns Swiss regulators may hold about the adequacy of the Swiss-U.S. Privacy Shield Framework, it is likely that similar concerns exist and that both Privacy Shield programs will share the same fate. Swiss and U.S. regulators will hold their annual review of the Swiss-U.S. Privacy Shield Framework in just over a month, on October 20, 2018.

Standard Contractual Clauses

Besides the Privacy Shield Frameworks, standard contractual clauses are another commonly used cross-border data transfer mechanism. Standard contractual clauses are model contracts that meet EU requirements for the protection of personal data being transferred outside the EU and EEA, and are used by thousands of organizations to conduct business in the EU and EEA. Like the Privacy Shield Frameworks, the adequacy of standard contractual clauses is being challenged and their future is uncertain.

In a long-fought battle between Max Schrems and Facebook, Inc. over Facebook's data transfer policies and practices, the Supreme Court of Ireland decided on July 31, 2018 to hear Facebook's arguments supporting its use of standard contractual clauses as a cross-border data transfer mechanism. Schrems has argued that Facebook has failed to adequately protect the personal data of EU citizens through its use of standard contractual clauses. Because the U.S. has less stringent privacy and data protection laws than the EU, critics of these clauses believe that their use permits improper transfer of the personal data of EU citizens to the U.S. By the end of 2018, the Supreme Court of Ireland is expected to review Schrems' challenge to the validity of this commonly used mechanism.

If EU court and regulatory efforts to invalidate standard contractual clauses and the Privacy Shield Frameworks continue to intensify and result in the suspension of these mechanisms, many U.S. organizations will be left without a practical means of transferring personal data to the U.S. from the EU, EEA, and Switzerland. Don't delay – now is the time to be proactive and consider what your organization will do if these data transfer mechanisms are invalidated.

If you have any questions about standard contractual clauses, the Privacy Shield Frameworks, cross-border data transfers, or the CLOUD Act, including how they may impact your organization, please contact any member of Baker Donelson's Data Protection, Privacy, and Cybersecurity Team.