COHEN & GRESSER

June 1, 2016

Grim Future for Transatlantic Personal Data Transfers: Model Clauses and the Privacy Shield in Jeopardy

Karen H Bromberg, Partner
Duane A Cranston, Associate

The Safe Harbor Framework, an agreement which thousands of multinational companies used to transfer personal data between the EU and the US without breaching the EU's strict data protection rules, was invalidated last October by the EU Court of Justice (CJEU) in the *Schrems* case. Following the collapse of this framework, many business entities entered into standard contractual clauses like Model Clauses and Binding Corporate Rules (BCRs) to effect transatlantic transfers of personal data to the United States.

In an earlier alert, we opined that the CJEU's rationale for striking down the Safe Harbor Framework – namely, the alleged large scale access to private data enjoyed by U.S. intelligence agencies – seemed at least potentially applicable to Model Clauses and BCRs as well, and warned that companies relying on these mechanisms should expect future legal challenges. It appears that time has come.

Just last week, the Irish Data Protection Commissioner announced its intention to seek declaratory relief in the Irish High Court and a referral to the CJEU to "determine the legal status of data transfers under standard contractual clauses." This announcement was precipitated by the filing of an amended complaint by Max Schrems, the privacy activist responsible for the collapse of the Safe Harbor Framework, in which he challenged Facebook's continuing transfer of his personal data. In this complaint, Schrems asserts that Model Clauses, and in particular Facebook's reliance on these clauses to allow its Irish subsidiary to transfer his personal data to its U.S. parent company, do not provide EU citizens with adequate means to seek relief to the extent required under EU law if a citizen discovers that a U.S. governmental agency has tapped into their data.

Schrems' challenge also places a renewed focus on the "Privacy Shield" agreement reached by EU agencies and the U.S. government this February. EU privacy laws restrict the export of their citizens' personal data to those countries which provide an adequate level of privacy protection. EU law considers data privacy protections to be inadequate in the U.S. and thus prohibits the transfer of personal information. The Privacy Shield is intended to address these legal requirements by imposing stronger data protection obligations on U.S. companies in order to align them with EU standards and remedy the deficiencies found by the CJEU in the Safe Harbor framework. The Privacy Shield is scheduled to be voted upon for ratification in June.

However, the Privacy Shield agreement is not without its own obstacles. Several EU privacy groups, including the Article 29 Data Protection Working Party, have criticized aspects of the plan, including the continuing right of the U.S.

government to collect or monitor personal information under certain circumstances. Earlier this week, the European Data Protection Supervisor issued an opinion stating, in part, that "the Privacy Shield as it stands is not robust enough to withstand future legal scrutiny before the Court." The supervisor noted that improvements would be needed to address "key data protection principles with particular regard to necessity, proportionality and redress mechanisms."

While neither of these developments has any immediate effect, they highlight the continuing uncertainty that companies face with respect to personal data transfers from the EU to the U.S. Companies should continue to closely monitor these developments and work with legal counsel to implement contingency measures in the event that either or both of these data transfer frameworks are invalidated by the EU data protection agencies.

About the Authors

Karen Bromberg is the head of the firm's Intellectual Property and Technology group. Karen is a Certified Information Privacy Professional (CIPP) with certifications covering both U.S. and European privacy law. She advises clients on a broad range of privacy and data protection matters, including privacy policies and procedures, regulatory investigations, global compliance, crossborder data transfers, cybersecurity and network intrusion issues, and contractual issues involving privacy and security with an emphasis on litigation avoidance.

Contact Karen

Duane Cranston serves as outside general counsel for a number of early to mid-stage companies in industries ranging from technology to healthcare, representing clients in data privacy, intellectual property licensing, commercial transactions, and employment matters. He counsels employers on employment issues including the development of employment policies related to insider trading and data privacy. Duane is a Certified Information Privacy Professional/United States (CIPP/US) through the International Association of Privacy Professionals.

Contact Duane

June 1, 2016

About Cohen & Gresser:

We are an international law firm with offices in New York, Paris, Seoul, and Washington, D.C. Founded in 2002, we have been recognized in Chambers USA, Legal 500, and Benchmark Litigation , and have grown to nearly sixty lawyers in six practice areas: Litigation and Arbitration, Intellectual Property and Technology, White Collar Defense, Corporate, Tax, and Employment Law.

New York | Paris | Seoul | Washington DC