Morgan Lewis

BLOG POST

TECH & SOURCING @ MORGAN LEWIS

TECHNOLOGY, OUTSOURCING, AND COMMERCIAL TRANSACTIONS
NEWS FOR LAWYERS AND SOURCING PROFESSIONALS

Dr. Axel Spies Discusses Recent Executive Order on Safeguarding Personal Information

October 25, 2022

AUTHORS
Dr. Axel Spies, Ksenia Andreeva, Kelli A. Boyle

SPOTLIGHT

US President Joseph Biden issued an Executive Order On Enhancing Safeguards for United States Signals Intelligence Activities on October 7, which establishes safeguards relating to the handling of personal information in the course of signals intelligence activities. In this edition of our Spotlight Series, we welcome Morgan Lewis special legal consultant Dr. Axel Spies, based in Washington, DC, to discuss the scope of this Executive Order and its implications.

How did this Executive Order come about?

This Executive Order is a response to the Court of Justice of the European Union's (CJEU) decision that the previous framework governing transatlantic data flows, the EU-US Privacy Shield, did not adequately protect EU personal data. In that case, known as Schrems II, the court's decision was based largely on the ability of the US government to collect personal data from Europeans combined with the lack of judicial redress available to them in the United States. Since the invalidation of the Privacy Shield by the CJEU in 2021, organizations that send personal data between the European Union and the United States must rely on more cumbersome methods for data transfer, such as revised lengthy Standard Contractual Clauses and Binding Corporate Rules, combined with laborious data transfer impact assessments. Thus, this Executive Order is an important step to restore data flows through a new Trans-Atlantic Data Privacy Framework by providing additional protections to European residents.

What does this Executive Order achieve?

There are two main achievements with the Executive Order. First, the Order requires signals intelligence, the surveillance of foreign electronic communications, to be "necessary" and "proportionate" to the "advancement of a validated intelligence priority." Necessity and proportionality are important concepts in EU law, enshrined in the Charter of Fundamental Rights of the European Union. They are also used in the recent California data protection regulations. And for an intelligence objective to be legitimate, it must fall under one of the enumerated categories, such as assessing terrorist organizations and global health concerns. At the same time, signals intelligence cannot be conducted based on a prohibited purpose, like

suppressing free speech, discriminating against people based on membership in certain protected classes, or collecting trade secrets unrelated to national security.

The Order also establishes a "two-layer redress mechanism, with independent and binding authority." In the first layer, EU individuals can file complaints with the Civil Liberty Protection Officer, housed within the Office of the Director of National Intelligence. Then, they can appeal decisions to the new Data Protection Review Court (DPRC) within the Executive Branch. The DPRC will select a "special advocate" in each case to advocate regarding the complainant's interest in the matter. But this new system only kicks in if the US Attorney General "designates a country or regional economic integration organization as a qualifying state for purposes of the redress mechanism established pursuant to section 3 of this order."

Are there any issues related to cross-border transfers of personal information that may be triggered by this Executive Order?

If the new system will be in place, data exporters should have to rely less on the more stringent and bureaucratic EU Standard Contractual Clauses (SCCs) or the "derogations" in the General Data Protection Regulation (GDPR), such as individual consents etc. in narrowly defined situations, to transfer personal data from the European Union to the United States. The main reason for the invalidation of the Privacy Shield was the surveillance of communications, over which corporations do not have much control. A lot has happened in the United States, also from the legal side, since 2006 when Snowden leaked his information on surveillance. The Executive Order should hopefully accommodate the concerns of the CJEU in terms of cross-border transfers of information. Whether it addresses all of the European legal concerns remains to be seen. Of course, organizations will also have to comply with all other relevant aspects of European data protection law. This means that the data importers together with the data exporters will still have to perform data transfer impact assessments for bringing personal data into the United States as before the Executive Order under Schrems II.

Do you anticipate any GDPR-related implications?

The new SCCs need to be in place by December 27. Therefore, there will be a legal gap between this data and March 2023 when we expect the Adequacy Decision of the European Commission. Article 45 GDPR allows for the transfer of personal data to countries outside the EU based on an adequacy decision by the Commission regarding the data protection regime of the United States. So the next step will be for the Commission to finish this process. What happens then is everyone's guess. While the CJEU could again declare an adequacy decision invalid, this new framework is the result of extensive negotiations, using Schrems II as guide. Mr. Schrems and his organization NOYB will likely file a lawsuit again. But it could take a long time before this lawsuit will wind its way through the courts with new facts and changes of the law being carefully evaluated by the judges. And we need to see how the new redress system will work in practice.

Topics: **Data Rights**, **Privacy**, **Spotlight**

Read more from Tech & Sourcing @ Morgan Lewis