Updates
October 10, 2022
President Biden Issues Executive Order Regarding Signals Intelligence Activities, Clearing Way for New Trans-Atlantic Data Privacy Framework

President Biden issued an executive order (EO) increasing protections and safeguards for personal data subject to signals intelligence activities. It also establishes a redress mechanism for residents of qualifying states who allege they were harmed by U.S. signals intelligence activity conducted in violation of U.S. law. The EO is intended to address perceived deficiencies in U.S. surveillance law identified by the Court of Justice of the European Union (CJEU) in its July 16, 2020 judgment (*Schrems II*) and to establish protections under U.S. law for personal data equivalent to those provided by the European General Data Protection Regulation (GDPR). The EO has been expected since the United States and the European Commission entered into an agreement on a Trans-Atlantic Data Privacy Framework in March of 2022. It places EU-to-U.S. data transfers on more solid footing under European Union (EU) law and is expected to support a new finding by the European Commission that the United States is among the handful of jurisdictions globally that provides adequate protection to personal data transferred from the EU.

Background

The GDPR, which entered into effect in 2018, imposes what many consider to be the most rigorous data privacy rules in the world. It protects personal data by recognizing individual rights related to data processing and security, laying down rules for when and how data may be processed or transferred, and authorizing the imposition of fines for infringement.

The GDPR reaches beyond the EU and regulates transfers of covered personal data to non-EU countries (third countries). Data may be transferred to a third country pursuant to a small handful of "lawful transfer mechanisms." One such mechanism permits transfer if the European Commission decides that the country's laws

provide an "adequate level of protection" of European personal data. If the EU Commission finds that a third country meets that standard in an "adequacy decision," businesses may then lawfully transfer data in reliance on that decision.

If the EU Commission determines that a third country's laws do *not* provide adequate protection for data, a business may only transfer data to that third country if it provides "appropriate safeguards." The GDPR allows for the use of binding corporate rules (BCRs) or Standard Contractual Clauses (SCCs) that are preapproved by the commission to satisfy this requirement, complemented by supplemental measures, if the data exporter determines in conjunction with the data importer that the specific data being transferred can be adequately protected.

The EU has repeatedly found that U.S. protections for personal data are not "adequate" because of the gap the EU perceives between the protection U.S. law provides and what the GDPR requires. The CJEU invalidated the original mechanism that the United States established for transatlantic data transfers, known as Safe Harbor, in 2015 after finding that U.S. laws governing foreign intelligence surveillance did not adequately protect European personal data. In response to that decision, the United States and the European Commission developed the Privacy Shield framework. The CJEU found the Privacy Shield framework deficient in 2020 in *Schrems II*. In particular, the CJEU found that Privacy Shield could not provide adequate protection because of perceived ongoing deficiencies in U.S. national security surveillance laws. With Privacy Shield stricken down, businesses were required to perform transfer impact assessments to determine whether other lawful transfer mechanisms, supported by supplemental measures, might adequately protect transferred personal data. The EO is intended to address the perceived deficiencies in U.S. law outlined in *Schrems II* by the CJEU. In the short term, businesses conducting transfer impact assessments should find it easier to determine that they can adequately protect transferred data. In the long term, the EO is expected to support a new European Commission adequacy finding undergirding a new EU-U.S. privacy framework that will simplify data transfers to the United States.

What the EO Seeks To Address

In *Schrems II*, the CJEU found insufficient limitations or safeguards to protect European data against U.S. surveillance. More specifically, the CJEU found that Section 702 of the Foreign Intelligence Surveillance Act (FISA) and Executive Order 12333 (EO 12333) allowed for the collection of or access to European data without sufficient safeguards and in instances in which such surveillance was not strictly necessary to protect national security. The CJEU also found that U.S. law failed to provide effective redress to European data subjects who alleged that their privacy was harmed by U.S. surveillance because they could not seek a remedy from an independent and impartial tribunal.

The Executive Order

The EO directly addresses the perceived deficiencies that the CJEU identified in *Schrems II*. It provides greater clarity regarding when the United States can conduct signals intelligence activities, introduces additional safeguards and protections for personal data, and establishes a new two-tier redress mechanism accessible to the residents of qualifying states who allege they have been subject to surveillance in violation of U.S. law.

New Safeguards

The EO establishes two important new safeguards for personal data affected by signals intelligence activities.

First, it permits the U.S. Intelligence Community (USIC) to conduct signals intelligence activities only to advance one or more of twelve specifically identified legitimate national security objectives. It ensures that signals intelligence activities will be proportionate by explicitly limiting intelligence activities to those that are "proportionate to the validated intelligence priority for which they have been authorized."

Second, it requires that the USIC appropriately consider "the privacy and civil liberties of all persons, regardless of their nationality or where they might reside" when conducting signals intelligence activities. It also extends to non-U.S. persons safeguards and protections previously enjoyed only by U.S. persons regarding the collection, use, dissemination, and retention of personal data.

Redress

The EO establishes a new two-tiered mechanism to review complaints by residents of qualifying states alleging that they were subject to surveillance in violation of U.S. law. In the first level of review, the Civil Liberties Protection Officer of the Office of the Director of National Intelligence (CLPO) will determine whether a "covered violation" has occurred, i.e., whether the complainant was subject to signals intelligence that violated U.S. law and "adversely affects the complainant's individual privacy and civil liberties interests." If the CLPO finds that a covered violation occurred, then it will determine an appropriate remedy that fully addresses any unlawful processing of the complainant's personal data. The CLPO will inform the complainant that "the review either did not identify any covered violations or the [CLPO] issued a determination requiring appropriate remediation."

Either the complainant or an affected USIC element may apply for the new Data Protection Review Court (DPRC) to review the CLPO's determination. The DPRC will consist of at least six judges appointed by the Attorney General. The EO includes several provisions designed to ensure that the DPRC is independent. For instance, it requires that the "Attorney General shall not interfere with a review by" the DPRC and that no judge shall be removed from the court except for instances of "misconduct, malfeasance, breach of security, neglect of duty, or incapacity."

Each application will be reviewed by a three-judge panel. To assist with the review and ensure the complainant's interests are fully represented, the DPRC must assign a "special advocate." The DPRC will determine whether a violation of U.S. law occurred and, if it did, whether the remedy required by the CLPO was appropriate. Upon completion of its review, the DPRC will inform the complainant that "the review either did not identify any covered violations or the [DPRC] issued a determination requiring appropriate remediation." CLPO determinations and DPRC decisions are binding on all elements of the USIC.

Implementation

The EO immediately has the force and effect of law and is binding on the USIC. It requires that a process for receiving complaints be established within 60 days of the date the order was issued. In order for data subjects to be allowed to submit a complaint to the CLPO, they must reside in a country that the Attorney General designates as a "qualifying state." It also requires the Attorney General to appoint DPRC judges and special advocates.

Takeaway

The EO addresses each perceived deficiency the CJEU identified in U.S. surveillance law. Companies relying on BCRs or SCCs should update their transfer impact assessments to account for the new safeguards and protections the EO creates within U.S. law. The European Commission has indicated its intent to "prepare a draft adequacy decision, as well as launch its adoption procedure." Once that process is complete and new EU-U.S. Data Privacy Framework principles are in place, participating companies will also be able lawfully to transfer personal data from the EU to the United States on the basis of the adequacy decision and Framework principles.

Authors

Explore more in

Privacy & Security | Technology Transactions & Privacy Law | National Security | Data Security Counseling and Breach Response | Communications | Digital Media & Entertainment, Gaming & Sports

Related insights

Update

DOJ's Final Rule on Data Transfers: Impacts Across Industries

Update

CFPB Proposes Rule To Expand Regulation E to Crypto and Gaming Accounts