CLIENT ALERTS & INSIGHTS

President Biden Enacts New Executive Order On EU-US Data Flow Agreement; EU Adequacy Decision Forthcoming

OCTOBER 10, 2022

The Executive Order hopes to address what had been shortcomings in the previous Safe Harbor and Privacy Shield programs that were struck down by EU courts in 2015 and 2020 respectively. On October 7, 2022, President Biden enacted the Executive Order On Enhancing Safeguards for United States Signals Intelligence Activities. The Executive Order seeks to address the biggest concern that EU courts have cited in striking down the previous EU-US data flow agreements: the inability of individual data subjects to exercise their rights under EU law over US government collection of their personal information.

The Executive Order comes over six months after the new EU-US data transfer agreement was announced in March 2022 (the "**Data Transfer Agreement**"). The Data Transfer Agreement is aimed at allowing for the simpler and lawful transfer of EU personal data to locations within the US. Once in place, the new Data Transfer Agreement will provide US-based entities with a new legal mechanism (other than cumbersome standard contractual clauses) to comply with the EU's General Data Protection Regulation ("**GDPR**").

Businesses and privacy advocates alike have been awaiting further details on the Data Transfer Agreement. As such, the details of the Data Transfer Agreement are key to understanding the possible legal longevity of the new Data Transfer Agreement, as EU courts have struck down similar agreements in the past. The original announcement was vague and scant on details; so, the Executive Order is the first window into that detail.

In line with the announced Executive Order, the EU announced it would begin the process of adopting an adequacy decision, which if successful, would mean the EU will would formally recognize the US as providing adequate data protection, sufficient to meet the rights granted to EU individuals under the GDPR. Such a decision would allow for the free flow of personal information across the Atlantic; something businesses have been lobbying for.

Obtaining an "adequacy status" would be a marked shift from the current legal landscape surrounding EU-US data flows as businesses would no longer need to rely on cumbersome standard contractual clauses in order to enter into to share personal data. This could possibly speed up the contracting processes between businesses and their vendors, make data transfers between affiliates and related entities of international businesses simpler, and help maintain the lawfulness of commonplace analytics and personalized advertising services.

EU and GDPR Legal Requirements

In order to lawfully transfer data under the GDPR from a location within the EU to a location outside of the EU, an entity must either (1) be sending the personal data to a country that the EU Commission has determined provides "adequate" safeguards equivalent to those in the EU; or (2) making the transfer subject to appropriate safeguards. Those safeguards can take the form of Standard Contractual Clauses ("**SCCs**"), binding corporate rules, or additional contractual safeguards. The new Data Transfer Agreement will be in place to assure that transfers of personal data from the EU to the US are subject to appropriate safeguards and comply with the second option.

Prior to July 2020, data transfers between the US and EU were subject to Privacy Shield, which was set up between the US and EU to ensure that the US provided adequate safeguards for data transfers. Numerous entities utilized Privacy Shield in order to properly transfer personal data from locations within the EU, to locations in the US without running afoul of the GDPR or EU Data Protection Authorities ("**DPAs**"). However, Privacy Shield was rejected by the EU courts in 2020.

Diplomats from both the EU and US have been working for years on a new agreement meant to both assure that individual privacy rights and freedoms of Europeans are upheld, and to allow the free flow of the technology trade (and with it, personal data) to continue between the EU and the US This effort represents the culmination of those negotiations, which began in the aftermath of the EU court's decision to strike down Privacy Shield.

EU-US Data Flow Background

In *Schrems II*, the Court of Justice of the European Union famously struck down the EU - US Privacy Shield. The main concern and issue raised by the court was that US law (and Privacy Shield) did not grant sufficient protection to an individual's privacy as compared to the GDPR. Specifically, the court was most concerned with unauthorized federal government access to personal data under the Foreign Intelligence Surveillance Act ("**FISA**"), and the lack of measures in place for European citizens to challenge such access or government requests.

The Court also called into question the validity of the old SCCs. The SCCs are a contractual tool that entities use to ensure that personal data shared over the course of a cross-border contractual relationship is properly protected and the rights guaranteed to European individuals are upheld.

While cumbersome, the SCCs have become a common mainstay in transactions that involve data transfer from the European Economic Area ("**EEA**") to other geographical locations. To address the concerns the Court raised in *Schrems II*, the European Commission adopted the new SCCs, which have been in place since this past summer and required since this past fall.

The development of a new Data Transfer Agreement is immensely important for the US and EU trans-Atlantic data flow relationship. Recently, DPAs ruled that data transfer relationships pursuant to the use of Google Analytics were unlawful under the GDPR. This underscores a recent trend of DPAs to move towards a data localization requirement under the GDPR.

The New Executive Order

When the Data Transfer Agreement was announced, President Biden indicated that the forthcoming Executive Order would provide individuals located in the EU with new legal avenues through which they could protect their privacy and exercise the rights granted to them under the GDPR.

Following through on that promise, the Executive Order establishes the Data Protection Review Court, which will be housed in the US Department of Justice. The Data Protection Review Court allows individuals to file claims against US government agencies. Individuals who make such claims will have a "special advocate" appointed on their behalf, and through the special advocates, the individual can attempt to limit the agency's collection and use of their personal information.

The Civil Liberties Protection Office will review complaints and then make referrals to the Data Protection Review Board, which will be a panel made up of judges appointed by the Attorney General. Decisions made by the Data Protection Review Court will be independent of the agencies it seeks to regulate (as it is housed under the Department of Justice and will be binding.

Importantly, individuals can use the Data Protection Review Board and the Executive Order complaints process as a "check and balance" on the FISA court process (used heavily by the US intelligence agencies) and use of their information gathered through US intelligence processes-the main issue that led to the EU courts striking down previous data transfer agreements.

On top of a new redress mechanism, the Executive Order also adopts data protection principles that are now commonplace under the GDPR and many other data protection laws-both under state law and international law. Data minimization-collecting only the information necessary for a specified purpose; only using it for the specified purpose; and only retaining it for the necessary time period-is an important data protection principle under the GDPR and the Executive Order makes that clear.

The Executive Order requires all intelligence agencies to establish and comply with policies and procedures "designed to minimize the dissemination and retention of personal information collected through signals intelligence."

Those policies must include requirements that retention of personal information is only allowed "if the retention of comparable information concerning United States persons would be permitted under applicable law and shall subject such information to the same retention periods that would apply to comparable information concerning United States persons." Further, the Executive Order requires agencies to delete non-US persons' personal information collected through signals intelligence that would have been deleted if the information was regarding a US person.

The newly established Privacy and Civil Liberties Oversight Board will be tasked with reviewing the adequacy of such policies and procedures.

Moving Forward

With the exponential increase in technology and software-as-a-service contracts, any US-based entity that does business in the EU or collects, transfers, or processes EU personal data will need to stay tuned for further updates as the new Data Transfer Agreement, once finalized, could allow a more efficient process to transfer applicable data.

The new Data Transfer Agreement will likely be an important tool for any and all contracts that contemplate the transfer of EU personal data to locations within the US

As the new trans-Atlantic data flow relationship between the US and EU evolves and more details come out with regard to the new Data Transfer Agreement, the Benesch Data Protection and Privacy team is committed to staying at the forefront of knowledge and experience to assist our clients in compliance efforts. We are available to assist you with any compliance needs.

Lucas Schaetzel at lschaetzel@beneschlaw.com or 312.212.4977.