LAW360

Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

US Privacy Changes Put EU Data Flow Pact On Strong Footing

By **Allison Grande**

Law360 (October 7, 2022, 11:37 PM EDT) -- The Biden administration's new commitments to enhance privacy protections for European Union residents whose personal data is swept up by U.S. intelligence-gathering activities elevates the latest version of a much-maligned transatlantic data transfer pact to the best position yet for survival, experts say.

In an attempt to address government surveillance and judicial redress concerns that led to the demise of the Privacy Shield data transfer framework two years ago, President Joe Biden signed an executive order Friday implementing the EU-U.S. Data Privacy Framework, which bolsters privacy and civil liberties safeguards for U.S. intelligence efforts involving personal data transferred from the EU to the U.S. and creates a multilayered, independent judicial mechanism for EU residents to challenge these activities.

Experts question whether President Joe Biden's executive order implementing the EU-U.S. Data Privacy Framework is enough to satisfy the European Court of Justice. (iStock.com/KanawatTH)

The changes are designed not only to provide the European Commission with a basis to adopt a new "adequacy" determination, which is required for the newly created Data Privacy Framework to officially take effect, but also to insulate the deal from meeting the same fate of its two predecessors, which were both deemed inadequate by the European Court of Justice.

"The executive order contains a really impressive set of privacy commitments from the U.S. government as well as creates a new [judicial] remedy clearly designed to meet the concerns that the Court of Justice raised," said Aaron Cooper, vice president of global policy at BSA: The Software Alliance. "We're hopeful and optimistic that the European Commission and Court of Justice view it that way too."

Experts agreed that the new executive order offers the most robust privacy and surveillance protections for EU personal data that the U.S. has ever committed to, with Bob Litt, global risk and crisis management co-chair at Morrison Foerster LLP, noting that the federal government has appeared to have "made a good faith effort to go as far as it can on this."

"This executive order is clearly an effort on the part of the U.S. to meet the European Court of Justice's

concerns in a way that's consistent with our legal framework and our need to protect national security," said Litt, who previously served as general counsel for the U.S. director of National Intelligence.

Still, questions continue to swirl about whether the U.S. government has done enough to narrow the scope of permissible surveillance or set up an adequate forum for judicial redress to be able to withstand yet another round of legal scrutiny, said Greg Nojeim, senior counsel and director of the security and surveillance project at the Center for Democracy and Technology.

"It remains uncertain whether EU authorities — and ultimately the EU Court of Justice — will deem these steps sufficient to satisfy the legal requirements for a new adequacy decision to support transatlantic data flows," Nojeim said.

Max Schrems, the Austrian privacy activist who mounted the legal actions that led to the fall of both the Privacy Shield and its predecessor Safe Harbor framework, has already vowed to challenge the validity of the new Data Privacy Framework.

In a statement Friday, Schrems predicted that the executive order is "unlikely to satisfy EU law," arguing that it continues to allow for bulk surveillance and establishes "a 'court' that is not an actual court."

Under the executive order, U.S. intelligence-gathering activities that sweep up EU residents' transferred data must be conducted "only in pursuit of defined national security objectives," take into consideration the privacy and civil liberties of all individuals involved, and be carried out "only when necessary to advance a validated intelligence priority and only to the extent and in a manner appropriate to that priority."

Additionally, the order puts the civil liberties protection officer at the Office of the Director of National Intelligence in charge of handling surveillance complaints lodged by EU residents, with any decision that the protection officer makes then being reviewed by an independent Data Protection Review Court that the U.S. attorney general is tasked with establishing and staffing with judges from outside the federal government.

But Schrems has contended that the EU and U.S. appear to have different ideas about what constitutes "necessary" and "proportionate" data collection and its use by intelligence authorities, and that "renaming some complaints body a 'court' does not make it an actual court."

However, despite the looming threat of another bruising legal challenge, there are some positive signs from Friday's developments for companies that have been clamoring for a Privacy Shield replacement, experts say.

"Since the announcement of the new EU-U.S. Data Privacy Framework in March, the pressure has been on the Biden administration to deliver an executive order that addressed the surveillance and redress concerns that are the primary concerns of EU authorities," said Ezra Church, a partner at Morgan Lewis & Bockius LLP. "There's still lots more to go, but this is a really encouraging step forward."

In response to the executive order, the EC issued a statement describing the measure as introducing "new binding safeguards that address all points raised by" the EU high court and stressing its belief that the Data Privacy Framework won't follow the same path as its predecessors.

"The objective of the Commission in these negotiations has been to address the concerns raised by the Court of Justice of the EU in the Schrems II judgment and provide a durable and reliable legal basis for transatlantic data flows," the commission said. "This is reflected in the safeguards included in the Executive Order, regarding both the substantive limitation on U.S. national security authorities' access to data (necessity and proportionality) and the establishment of the new redress mechanism."

Companies have been anxiously awaiting progress on a new data transfer policy since the U.S. and EU earlier this year reached an "agreement in principle" on the Data Privacy Framework to replace the Privacy Shield, which more than 5,300 multinationals had relied on to legally transfer data between the regions before it was invalidated.

That decision threw the transatlantic data transfer landscape into uncertainty, with companies left to rely on existing alternative transfer mechanisms known as standard contractual clauses and binding corporate rules, both of which require more legwork to implement than certifying compliance to Privacy Shield. The contractual clauses are legal agreements between one sender and one receiver about how transferred data will be handled, while binding corporate rules can only be used for transferring data within a corporate unit and require regulatory approval.

But the commission's apparent support of the U.S. commitments made in the executive order and its pledge to begin the process of reviewing the adequacy of the deal, which is expected to take until at least the spring, "really puts an EU stamp of approval on this as the adequacy process plays out," said Caitlin Fennessy, vice president and chief knowledge officer at the International Association of Privacy Professionals.

While privacy pros can't rely on the adequacy decision yet, they can now "breathe a little easier" as the latest developments provide "a lot of assurance" that the EC thinks the U.S. commitments and new data transfer framework meet the adequacy standard, according to Fennessy, who formerly served as Privacy Shield director at the U.S. International Trade Administration.

"[The invalidation of Privacy Shield] caused havoc for major U.S. tech firms in Europe, but led mainly to confusion, higher legal costs, and a limited selection of service providers for smaller firms," Fennessy added. "Today's executive order and [accompanying] Department of Justice regulations change this context, providing new protections aimed at rebuilding trust and trade across the Atlantic."

For EU authorities, "the devil may be in the details" when it comes to evaluating the strength of the executive order, which contain directions to the DOJ, the Office of the Director of National Intelligence, and others within the U.S. government "to set up various and multi-layered processes to limit surveillance and provide review and redress for the claims of individuals," said Church, the Morgan Lewis partner.

"Those things will take time to implement," Church added.

But the federal government is likely to "move quickly" to establish those safeguards, particularly the ones involving the new Data Protection Review Court, because it will want to show the EC as it weighs its adequacy decision that these mechanisms are "up and running," predicted Litt of Morrison Foerster.

"It's definitely manageable and doable from the U.S. side," Litt added. "What's unclear is whether the European Court of Justice will find it acceptable."

While the Court of Justice's decision didn't flag any concerns with how companies are handling and transferring consumer data, the framework's commercial principles are unlikely to be identical to Privacy Shield, which means that companies that want to certify their compliance with the new mechanism will need to consider whether they need to make at least minor changes to their policy language and data practices.

Dona Fraser, senior vice president at BBB National Programs, said Friday that the organization and its global privacy division are prepared to help businesses that have opted to remain self-certified to Privacy Shield experience "a smooth transition" to the enhanced framework and whatever changes might be made to the commercial aspects of the mechanism, as well as to "welcome those businesses who have chosen to pause their Privacy Shield self-certification."

BBB will also continue to operate its long-running independent recourse mechanism, which provides both compliance assistance for businesses and free redress for EU residents who have complaints about how companies are transferring their personal data, according to Fraser.

"Hopefully, this announcement will encourage those that have stayed certified to remain and those that have left the program to consider rejoining it, because now there are some teeth to this again, and we're seeing the progress we needed to see," Fraser said.

While the extent to which companies will jump at the opportunity to use the new Data Privacy Framework remains unclear, they're likely to welcome the broader impact of Friday's executive order on their transatlantic data transfer practices.

In issuing the order, the Biden administration made clear its new "robust" privacy and redress commitments cover transatlantic data flows initiated not just under the upcoming framework but also under the alternative transfer mechanisms of the standard contractual clauses and binding corporate rules.

"This is huge, because companies have spent the last two years conducting their own assessments of national security protections for any data transfer mechanism," said Fennessy of the International Association of Privacy Professionals. "Now, this will make life easier for privacy professionals because they'll be able to point to these new binding legal rules in the U.S. that the EU is likely to agree will meet the standard the Court of Justice set to support these transfers."

--Editing by Jill Coffey and Michael Watanabe.
