October 13, 2022

White House Issues Executive Order Outlining Key Points of the Transatlantic Data Privacy Framework

Attorneys
Fran Faircloth
Rohan Massey
Edward McNicholas
David Peloquin
Christopher Foo
Edward Machin

On 7 October 2022, the White House issued an Executive Order, as well as an accompanying Fact Sheet, which sets out the foundations for the Transatlantic Data Privacy Framework ("Framework").

Since the decision of the Court of Justice of the European Union ("CJEU") in the Schrems II case in mid-2020, organizations have not been able to rely upon the Privacy Shield Framework to transfer data from the European Union ("EU") and other European Economic Area countries to the U.S. As a result, many have sought to rely on other data transfer mechanisms, the most common being the EU Standard Contractual Clauses ("SCCs"). However, the Framework would allow participating organizations to transfer personal data freely, removing the administrative and commercial burden of the SCCs.

The Executive Order addresses data privacy concerns raised by Schrems II through introducing, among other measures, further safeguards and oversight of personal data collection by U.S. signals intelligence ("SIGINT") activities and provides individuals with a redress mechanism for their data protection concerns. Although the Executive Order is a positive step forward, welcomed by many, the long-term durability of the Framework remains uncertain, and the Framework is not functional until the European Commission issues an adequacy decision based on the Framework, the timing of which remains uncertain.

Background

In March 2022, U.S. President Biden and European Commission President von der Leyen announced jointly that they had reached an agreement in principle on the long-awaited replacement to the EU-U.S. Privacy Shield framework. Since then, details have been scarce although it was clear that the new Framework would rely on the Privacy Shield Principles, safeguard individuals' privacy rights from unnecessary and disproportionate U.S. intelligence activities, and introduce a redress mechanism for individuals (for more information, please see our previous Alert). The Executive Order shows how the U.S. government intends to implement some of these measures into practice by translating and implementing its safeguards and redress commitments into U.S. law.

Summary of key provisions in the Executive Order

1) SIGINT Controls and Oversight

The Executive Order mandates that SIGINT activities be conducted only in pursuit of defined national intelligence objectives while taking into account the privacy and civil liberties of all persons regardless of nationality or country of residence. The Executive Order further provides that such activities take place only when necessary and in a proportionate manner that advances a validated intelligence priority. Such intelligence priorities are assessed through a defined process that requires input from the Civil Liberties Protection Officer of the Office of the Director of National Intelligence ("CLPO") to assess whether such priorities are "legitimate" and proportionate. SIGINT agencies are also required to update their policies and procedures to reflect the new privacy and civil liberties safeguards in the Executive Order, publish such documents "to the maximum extent possible, consistent with the protection of intelligence sources and methods", and designate senior-level "legal, oversight and compliance officials" with sufficient authority, resources and support to identify and remediate incidents of non-compliance with applicable U.S. law, such as the Executive Order.

2) Redress Mechanism

The Executive Order establishes a dual-layered mechanism for individuals to obtain review and redress for claims that their personal information was collected in violation of applicable U.S. law. Under the first layer, complaints that fulfill criteria and provide sufficient information will be reviewed by the CLPO and subject to an investigation; if the CLPO determines that the Executive Order's safeguards and/or other applicable U.S. laws have been violated, it may determine appropriate remediation measures. Such measures are binding upon intelligence community agencies, subject to the second layer of review. Under the second layer, the Executive Order provides for the establishment of a Data Protection Review Court ("DPRC") comprising judges with relevant data privacy and national security experience and qualifications to review cases independently. The DPRC is empowered to review the CLPO's decisions in the event of an application from individuals or from intelligence community agencies, and such reviews are binding upon the CLPO's decisions.

The redress mechanism will also be subject to annual review by the Privacy and Civil Liberties Oversight Board (an independent agency within the U.S. government), in particular to ensure whether qualifying complaints were processed in a timely manner and whether compliance with the Executive Order and CLPO/DPRC decisions was achieved.

Commentary

The Executive Order's emphasis on necessity and proportionality, as well as the need for signals intelligence activities to take place only in the presence of specified national security purposes and the availability of an individual redress mechanism, tracks the language of the *Schrems II* decision and is a clear attempt to address specifically the CJEU's main concern – namely, that U.S. national security legislation could overly interfere with an individual's rights to privacy and that the measures implemented under Privacy Shield were incapable of providing a level of protection "essentially equivalent" to that available under EU law.

However, it remains to be seen whether these measures will satisfy the CJEU in the event of a future legal challenge. Despite introducing requirements for necessity and proportionality, the Executive Order still permits the bulk collection of personal data, which was a major issue in *Schrems II*. The Executive Order does subject such bulk collection to tighter controls and permits it only when targeted data collection is not available. Furthermore, the DPRC, as an entity within the U.S. government's executive branch, may not be regarded as a "court" for the purposes of EU law. Under EU law, "courts" are established as a judiciary body separate from executive branches of government, similar to "Article III" courts in the U.S. There is thus uncertainty as to whether the DPRC, which is established expressly by the Executive Order and therefore arguably not separate from the executive branch, can provide "effective administrative and judicial redress".

Next steps and practical takeaways

The Executive Order forms the basis for the European Commission ("EC") to adopt a new adequacy decision to implement the Framework. The draft adequacy decision will be subject to review by the European Data Protection Board ("EDPB"). In addition, an EU committee comprising representatives from each EU member state must vote to approve the decision before it can be implemented. This process can be time consuming, as past adequacy decisions for other countries have taken anywhere between several months to several years to obtain approval, although previous comments by the EC have alluded to an aspirational implementation date within several months. Furthermore, if the EDPB's influential, albeit non-binding, opinion provides a negative outlook, or if privacy campaigners challenge the Framework, it may be subject to further revision and discussions between the U.S. and EU. It is also not clear whether the enhanced proportionality and redress measures provided in the Executive Order or final approval by the EC will serve to inoculate the Framework from invalidation through legal challenges, as was the fate of its two predecessors.

In the meantime, as the Framework has not yet been adopted as an adequacy decision by the EC, organizations must continue to rely upon existing data transfer mechanisms, such as the SCCs, and comply with their attendant obligations, such as data transfer impact assessments, to transfer personal data to the U.S. in a lawful manner. Although the measures in the Executive Order may be reflected in data transfer impact assessments conducted by parties transferring personal data from the EU to the U.S., the existence of the Framework alone will not be sufficient in and of itself to validate data transfers to the U.S., meaning that organizations must still carry out this assessment when relying on transfer mechanisms that require it. We are continuing to monitor this space for updates.

If you have any questions, please contact Fran Faircloth, Rohan Massey, Edward R. McNicholas, David Peloquin, Christopher Foo, Edward Machin, or your usual Ropes & Gray advisor.