HUNTON ANDREWS KURTH

Lawyer Insights

A New Era: The EU-U.S. Data Privacy Framework

By Sarah Pearce and Lisa Sotto
Published in Thomson Reuters' Regulatory Intelligence | July 26, 2023


The European Commission has formally adopted a new adequacy decision on the EU-U.S. Data Privacy Framework. The adoption of the adequacy decision had been eagerly awaited, following intense negotiations between the EU and the United States after the invalidation of the framework's predecessor, the Privacy Shield, by the Court of Justice of the European Union (CJEU) in the Schrems II decision in July 2020.

Under Article 45 of the General Data Protection Regulation (GDPR), personal data cannot be transferred outside of the EU unless the data is being transferred to a country deemed by the EU to provide adequate protection for personal data, or a transfer mechanism has been implemented, such as the European Commission's Standard Contractual Clauses (SCCs) or Binding Corporate Rules.

The CJEU, in both Schrems I and Schrems II, raised significant concerns regarding U.S. law that indicated the data protection standard in the U.S. did not meet the standard that was "essentially equivalent" to that in the EU. The CJEU highlighted in particular the issue of the U.S. government authorities' access to and use of EU personal data, notably (1) the fact that it was not restricted by the principle of proportionality, and (2) the lack of effective redress for EU data subjects to challenge any U.S. surveillance. In addition to invalidating the Privacy Shield, these concerns also led to the CJEU scrutinizing the SCCs available for use at the time, specifically how they were used in practice to ensure the adequate protection of personal data transferred to the United States.

Relief for organisations

In light of the Schrems II decision, the European Commission expedited its preparation of a new set of SCCs (which were in the process of being prepared to align with the GDPR) to deal with the issues raised by the CJEU. Although the new SCCs did address the concerns of the CJEU, the result was a new set of complicated and convoluted contractual clauses, with the requirement to conduct an extensive transfer risk assessment for each cross-border transfer. The implementation of the new SCCs plagued many organisations transferring data to the U.S. and the new framework will provide a much-needed measure of relief for those organisations.

Significant changes have been made to the relevant legal regime in the United States following Schrems II, most notably with respect to U.S. government surveillance activities. The U.S. has, by way of the Biden Administration's October 7, 2022, Executive Order 14086 on Enhancing Safeguards for United States Signals Intelligence Activities, put in place legal safeguards that limit access to personal data by its surveillance authorities to what is necessary and proportionate to achieve specific purposes, thus meeting the EU's proportionality requirement. It has also introduced more robust oversight and redress

mechanisms, such as the Data Protection Review Court, giving data subjects the right to challenge violations of the Framework.

The European Commission reviewed EO 14086 alongside the Schrems II judgment when preparing the framework's adequacy decision and, in its view, the changes made address all the key issues. The text of the adequacy decision itself concludes that the "United States ensures an adequate level of protection # comparable to that of the European Union # for personal data transferred from the EU to U.S. companies under the new framework."

Essential Equivalence

There is no question that a number of stakeholders will be scrutinizing — and challenging — the adequacy decision in weeks and months to come. Earlier this year, the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE) urged the Commission not to adopt adequacy based on the Framework on the basis that it "fails to create actual equivalence" with the EU in the level of data protection it provides. The European Data Protection Board (EDPB) has also highlighted certain points of concern, such as insufficient rights of access for data subjects to their personal data. Importantly, an adequacy finding does not require an identical level of protection; the requirement is "essential equivalence." This means that the third country in question can have a regime in place for protecting personal data that differs from that in the EU, as long as it effectively ensures an adequate level of protection. The test is whether, through the substance of privacy rights and their effective implementation, supervision and enforcement, the foreign system as a whole delivers the required level of protection.

While neither the LIBE nor the EDPB's opinions were binding, and the adequacy decision has since been formally adopted, the criticisms raised previously will provide ammunition to potential challengers and we should expect that the CJEU will, again, be asked to assess whether the new safeguards provided by the Framework are sufficient to be considered essentially equivalent to the safeguards in the EU.

In this regard, Mr. Schrems has already confirmed that he will appeal the framework's adequacy decision, stating that the "third attempt of the European Commission to get a stable agreement on EU-U.S. data transfers will likely be back at the Court of Justice (of the European Union) in a matter of months." In his view, the changes made to U.S. rules do not address fundamental surveillance issues or offer effective legal redress.

The official website for the framework went live on July 17, 2023, enabling self-certifications to begin from that date. Organisations that are currently Privacy Shield-certified will have access to a simplified procedure for self-certification and will be given three months to transition to the new framework. The list of certified organisations is available on the website, in the same way as they were for the Privacy Shield. The framework was intended to address national security issues rather than commercial concerns and, as such, the changes are not substantive. Indeed, the terms of the framework are very similar to that of the Privacy Shield; other than updating references to the new framework (rather than the Privacy Shield), transition to the new framework will be automatic for Shield-certified organisations provided they continue to comply with the framework's principles.

The Department of Commerce will be responsible for administering the framework, and in doing so will process applications for certification and monitor whether participating organisations continue to meet the certification requirements, including by performing random spot checks. Compliance by U.S.

organisations with their obligations under the framework will be enforced by the U.S. Federal Trade Commission.

Welcome news for UK

The framework's adequacy decision is also welcome news for UK organisations exporting data to the U.S. On June 8, 2023, the UK and U.S. governments announced a commitment in principle to establish the UK Extension to the framework, creating a "data bridge" between the two countries. According to the UK government, the bridge will remove the "burden" of putting in place "costly contract clauses . . . to ensure protection and privacy standards are maintained." Indeed, the idea is that U.S. organisations approved to join the framework would be able to receive UK personal data — in the same way they had under the Privacy Shield, without the need for additional, lengthy contractual provisions. There is no clear timeline, however, for the effective date of the UK Extension so, for the time being, the UK International Data Transfer Agreement and the UK International Data Transfer Addendum to the EU SCCs will remain the most appropriate means of transferring UK personal data to the U.S.

The successful negotiation of the new framework is a coup for the negotiators who were operating under a bright spotlight with many onlookers. While there is little question that challenges are forthcoming, the framework represents a critical step forward in easing the current complexity of EU-U.S. data transfers and should be heralded as a success.

A new era: The EU-U.S. Data Privacy Framework
By Sarah Pearce and Lisa Sotto
Published in Reuters | July 26, 2023

Sarah Pearce *is a partner in the firm's Global Technology, Outsourcing & Privacy group in the firm's London office. Sarah's practice covers a broad range of data privacy and data security issues in the UK and across Europe. She can be reached at +44 (0)20 7220 5722 or spearce@HuntonAK.com.*

Lisa Sotto *is chair of the firm's global privacy and cybersecurity practice group and managing partner of the firm's New York office. In her practice, she assists clients in identifying, evaluating and managing risks associated with privacy and data security practices, counseling them on a wide range of issues from U.S. state and federal privacy and data security requirements to security breach notification laws and global data protection laws (including those in the EU, Asia and Latin America). She can be reached at 212-309-1223 or LSotto@HuntonAK.com.*