Response by the Centre for Information Policy Leadership to the European Commission's Questionnaire for First Periodic Review of the EU – U.S. Data Privacy Framework

31 May 2024

INTRODUCTION

The Centre for Information Policy Leadership ("**CIPL**")[1] appreciates the opportunity to submit this response to the European Commission's Questionnaire for First Periodic Review of the EU – US Data Privacy Framework (the "**Framework**" or "**DPF**"). This response is based on CIPL's own substantial experience and observations in working with our member organizations and other stakeholders on global data transfer solutions, on the information CIPL received from member organizations in response to the Questionnaire, and on input from privacy counsel of the law firm of Hunton Andrews Kurth LLP ("**Hunton**") based on their experiences to date advising a diverse range of clients on compliance with, and certification to, the Data Privacy Framework (collectively "**Respondents**").

CIPL strongly supports the dedicated and cooperative work undertaken by the European Commission and the U.S. Department of Commerce to create this data transfer mechanism following the invalidation of the Privacy Shield. This new framework, with its binding safeguards and limits to data access by U.S. intelligence agencies to only those measures that are necessary and proportionate as well as the independent redress mechanism for Europeans, significantly strengthens the data protection interests of individuals and facilitates trusted transatlantic data transfers for organizations. The fact that the safeguards put in place by the US for the DPF also facilitate the use of other transfer mechanisms further lessens the otherwise disproportionate burden on organizations assessing risk of transfers to the US.

As an initial matter, CIPL notes that the invalidation of previous data transfer frameworks has heightened concerns among organizations whose business and core operational functions rely on the existence of stable data transfer mechanisms. Some of these organizations question whether the revised Data Privacy Framework will ultimately withstand a future court challenge, leading to hesitation by some organizations in adopting the new adequacy decision framework or holding off on certifying pending any court challenges. This has resulted in continued reliance on alternative data transfer mechanisms like Standard Contractual Clauses ("**SCCs**"). However, CIPL encourages the European Commission and the U.S. Government to ensure the continued functioning of the Data Privacy Framework. This framework has the

[1] CIPL is a global privacy and data policy think tank in the law firm of Hunton Andrews Kurth LLP and is financially supported by the law firm and 90+ member companies that are leaders in key sectors of the global economy. CIPL's mission is to engage in thought leadership and develop best practices that ensure both effective privacy protections and the responsible use of personal information in the modern information age. CIPL's work facilitates constructive engagement between business leaders, privacy and security professionals, regulators, and policymakers around the world. For more information, please see CIPL's website at http://www.informationpolicycentre.com/ Nothing in this submission should be construed as representing the views of any individual CIPL member company or of the law firm of Hunton Andrews Kurth.

potential to provide a more comprehensive and efficient data transfer mechanism than other existing mechanisms under the EU General Data Protection Regulation (GDPR).

Indeed, one of the key features of the Data Privacy Framework is that it can substantially mitigate the burdens and inefficiencies created by transfer-compliance obligations that too frequently are disproportionate to the actual risks associated with particular data transfers—a state of affairs described in a recent study by Professor Theodore Christakis.[2]

While some apprehension around the Framework's stability remains given the experience with its predecessor frameworks, CIPL nevertheless found organizations to support the Framework and their strong desire for its continued existence – not only as a valid a transfer mechanism, but also as a tool to demonstrate their accountability and data protection compliance to customers, business partners and regulators.

RESPONSES BASED ON EXPERIENCES OF CIPL, ITS MEMBERS, AND COUNSEL

1. **Certification under the Data Privacy Framework**

CIPL has 30 members that are (or have affiliates that are) certified under the Data Privacy Framework. In response to our outreach to members for this submission, we received responses from organizations that are either already certified under the Data Privacy Framework or plan to be certified in the near future.

Hunton has counseled approximately over 120 companies in connection with certifying to the Data Privacy Framework and its predecessor frameworks. This number includes affiliated entities that are certified as part of a parent company's certification. A majority of the companies counseled by Hunton with respect to Privacy Shield compliance chose to certify to the Data Privacy Framework. Hunton has also counseled or is counseling at least six companies who certified or are in the process of preparing to certify to the Data Privacy Framework and did not previously participate in the Privacy Shield.

Experiences around the functioning of the certification mechanism have been mostly positive: Respondents have found the requirements reasonable and noted that since the certification process under DPF is similar to Privacy Shield, the transition to the new framework has been smooth and efficient. In addition to the certification's core purpose of facilitating data transfers, as mentioned above, some Respondents view the certification as a valuable public "privacy seal", providing customers, business partners and regulators further assurances of sound data protection governance, accountability, and compliance.

"The 'Zero Risk' Fallacy: International Data Transfers, Foreign Governments' Access to Data and the Need for a Risk-Based Approach," February 2024, available here. The report was produced with support from CIPL.

2. Measures taken in application of the DPF Principles

Most of the Respondents to our survey are large multinational companies with robust global privacy programs. These organizations are required to comply with a variety of legal obligations related to notice, access, choice, data integrity, purpose limitation, security, and the rights of data subjects. Against this backdrop, several Respondents noted and appreciated that the principles of the Data Privacy Framework generally align with established global standards. For many, the principles of the Framework were already incorporated or mostly reflected in their existing privacy policies and processes. Therefore, only minor adjustments and updates were necessary to fully comply with the DPF standards.

Furthermore, where EU-approved Binding Corporate Rules ("BCR") were already in place, adopting the Data Privacy Framework required minimal adjustments to existing practices and transparency. The primary change centered around updating references in notices and policies from the Privacy Shield to the Data Privacy Framework.

As with the previous Privacy Shield Principles, Respondents have put in place privacy-specific internal compliance programs, oversight mechanisms and other measures including corporate policies and procedures, written guidelines on the implementation of such policies within the organization, training programs, and reporting channels to ensure the effective application and implementation of the Data Privacy Framework Principles.

Hunton has worked very closely with its clients to help them design robust and effective internal compliance practices to comply with the Data Privacy Framework's Principles and handle complaints that might arise. These measures include conducting due diligence regarding the organization's compliance with the Data Privacy Framework Principles (such as Security Principle due diligence), implementing Framework-specific policies and procedures setting forth how the organization will comply with the Data Privacy Framework Principles, training relevant personnel responsible for the organization's compliance with the Data Privacy Framework Principles or who otherwise are responsible for cross-border data transfers, and facilitating mechanisms to conduct the annual verification of the organization's compliance with the Data Privacy Framework Principles in connection with recertification.

3. Relationship with third parties

Generally, Respondents reported that they seek to comply with the Accountability for Onward Transfer Principle by executing onward transfer agreements with third parties and affiliates/subsidiaries (both controllers and processors) to whom they onward transfer EU personal data after receiving it in the United States. These agreements are designed to meet the requirements contained in the principle, including by requiring onward transfer recipients to provide at least the same level of privacy protection for personal data as is required by the Data Privacy Framework Principles through the full data lifecycle, and to stop the processing of the relevant personal data if they cannot meet this requirement.

Some Respondents have implemented specific technical and organizational measures to comply with the Accountability for Onward Transfer Principle. For example, one Respondent described regularly updating a list of "Third-Party Subprocessors", which lists all third parties authorized to access and process personal data to which they are given access via self-service portals with notification functionalities.

4. Complaint Handling

None of the Respondents have reported receiving any complaints or general inquiries from EU individuals concerning the transfer of personal information under the Data Privacy Framework.

5. Independent Dispute Resolution

Respondents have indicated that they use the Better Business Bureau (BBB) and Judicial Arbitration and Mediation Services (JAMS) as their trusted agents in the US for dispute resolution. However, to date, none of these dispute resolution mechanisms have been triggered.

6. Access to Data for National Security and Law Enforcement Purposes

The vast majority of Respondents have not received requests for access to data from law enforcement agencies. For those that have received such requests, this information is disclosed in their public transparency reports.

7. Other Information

Respondents expressed a strong desire to ensure that the Data Privacy Framework remains a stable and reliable data transfer mechanism. Previous experiences with the overturning of Safe Harbor and Privacy Shield mechanisms necessitated organizations to review, update, and redeploy contracts and processes that were based on these earlier frameworks, resulting in significant costs and administrative burdens. Therefore, some Respondents are cautious about relying exclusively on the Data Privacy Framework for day-to-day processing and are instead, or in addition, using a range of options, most notably the updated Standard Contractual Clauses together with enhanced technical and organizational measures to cover international transfers to the US.

CIPL urges the European Commission and the U.S. Government and Department of Commerce to continue to work toward effective implementation of the Data Privacy Framework, given its potential to serve as a sustainable, comprehensive, and efficient accountability and data transfer mechanism.