EU - U.S. Data Privacy Framework

First periodic review

Bruno Gencarelli
Head of Unit, International Affairs and Data Flows
European Commission
Rue Montoyer, 59
1000, Brussels

Brussels, 31 May 2024

Dear Mr. Gencarelli,

This document responds to your letter of 2 May requesting that the Computer & Communications Industry Association (CCIA) respond to a questionnaire to aid with the first periodic review of the EU - U.S. Data Privacy Framework. CCIA is an international, not-for-profit association representing a broad cross section of computer, communications, and internet industry firms.

In order to respond to this questionnaire, CCIA surveyed its member companies and received a number of responses describing their experiences with respect to the practical implementation of EU - U.S. Data Privacy Framework. CCIA's member companies' responses generally reflected the thorough and thoughtful nature of their efforts to protect the information of EU data subjects in a manner consistent with their obligations under the Data Privacy framework.

I. Certification experience under the Data Privacy Framework

10 CCIA member companies are certified under the EU - U.S. Data Privacy Framework. In 2020, 12 CCIA member companies were certified under the Privacy Shield. Of those who did not seek recertification, they rely on protections afforded in separate adequacy decisions, including the use of binding agreements or arrangements for onward transfers to entities situated in the United States.

II. Measures taken in application of the DPF Principles

Since all CCIA member companies that are certified under the DPF previously held a Privacy Shield certification, the implementation work required to prepare for the DPF was not significant. Several members reported conducting a gap assessment in order to identify and implement the work required to update all policies, procedures and contracts as required by the DPF. Members did not report any significant challenges when transitioning to the DPF Principles.

With regard to the Notice Principle, responding members maintain a public privacy policy and employee privacy policies for HR data, where HR data is covered. Responding members have notified their customers of these new DPF updates to their privacy policy and Data Processing Addendum through various means including email or a dedicated section on their service interface.

Responding members also maintain a data subject request (DSR) procedure in accordance with the Access Principle. This procedure informs the requester of their relevant data subject rights including instructions on ways to submit their requests.

III. Relationship with third parties

Respondent CCIA members comply with the Accountability for Onward Transfer Principle by requiring third parties to sign binding contractual agreements (e.g. data processing addendum) and adhere to the conditions for processing personal data under those agreements. Such conditions may consist of ceasing data processing or other appropriate measures in the event where third parties can no longer meet their contractual obligations.

Responding members carrying out onward transfers within the same group continue to establish and rely upon Binding Corporate Rules or Standard Contractual Clauses. Such binding measures may include for instance an obligation for the exporting entity to carry out a transfer impact assessment jointly with the importing entity, and identifying and implementing additional safeguards where necessary pursuant to the findings of said transfer impact assessment.

IV. Complaint handling

Respondent companies reported that they have yet to receive any complaints from EU individuals regarding the transfer of their personal information under the DPF.

V. Independent dispute resolution

Respondent companies use different independent Dispute Resolution programs (e.g. TRUSTe, VeraSafe, JAMS). However, members have received no complaints from EU individuals via dispute resolution bodies regarding the transfer of their personal information under the DPF.

VI. Access to data for national security and law enforcement purposes

The majority of member respondents include information on access requests by U.S. authorities for national security purposes in their transparency reports as permitted by the USA Freedom Act. These reports are typically updated on a biannual basis, subject to six month reporting delay.

For most responding companies, the total requests for U.S. national security purposes (FISA Court Orders, NSL) have numbered in the 0-249 band for the most recent reporting period. A minority of member companies are reporting national security requests within the range of 0-499. On average, the number of national security requests received remains steady to previous reporting periods. The vast majority of government access requests pertain to non-content data (e.g. subscriber information). While transparency reports are publicly available on member companies' websites, CCIA will not include individual transparency reports in order to protect the confidentiality and anonymity of member responses.

While CCIA is not in a position to supply the number of data access requests for criminal law enforcement purposes and conclusively identify patterns, respondent companies have

policies to, where legally permitted, provide notice to users prior to disclosing any information to law enforcement in compliance with a valid legal process.

Lastly, responding members have reported that they have not provided information in response to access requests for criminal purposes that they believe conflicted with EU law. However, the uncertainties between the US and the EU's respective government data access requests and privacy laws occasionally raise questions among customers and end-users. CCIA is aware that negotiations for an agreement to facilitate access to electronic evidence in criminal investigations are underway. We would welcome an agreement that establishes a framework for addressing potential concerns and helps reduce tensions and any uncertainties in this area.

VII. Other information

Respondent companies did not report encountering any challenges in implementing or operating under the EU - U.S. Data Privacy Framework.

Respectful submitted,

Alexandre Roure
Head of Policy, Deputy Head of Office
Computer & Communications Industry Association

Alvaro Marañon
Policy Counsel
Computer & Communications Industry Association

About CCIA Europe

The Computer & Communications Industry Association (CCIA) is an international, not-for-profit association representing a broad cross section of computer, communications, and internet industry firms.

As an advocate for a thriving European digital economy, CCIA Europe has been actively contributing to EU policy making since 2009. CCIA's Brussels-based team seeks to improve understanding of our industry and share the tech sector's collective expertise, with a view to fostering balanced and well-informed policy making in Europe.

For more information, visit: twitter.com/CCIAeurope or www.ccianet.org

CCIA is registered in the EU Transparency Register with number 281864052407-46.

For more information, please contact:

CCIA Europe's Head of Communications, Kasper Peters: kpeters@ccianet.org