UNITED STATES DEPARTMENT OF COMMERCE
International Trade Administration
Washington, D.C. 20230

July 13, 2023

The Right Honorable Chloe Smith MP
Secretary of State
Department of Science, Innovation and Technology (DSIT)
100 Parliament Street
London
United Kingdom
SW1A 2BQ

Dear Secretary of State Smith:

On behalf of the International Trade Administration ("ITA"), I am pleased to describe the commitments the Department of Commerce ("the Department") has made to ensure the protection of personal data through its administration and supervision of the Data Privacy Framework program. Finalizing the United Kingdom Extension to the EU-U.S. Data Privacy Framework ("UK Extension to the EU-U.S. DPF") is a major achievement for privacy and for businesses on both sides of the Atlantic, as it will offer confidence to UK individuals that their data will be protected and that they will have legal remedies to address concerns related to their data, and will enable thousands of businesses to continue to invest and otherwise engage in trade and commerce across the Atlantic to the benefit of our respective economies and citizens. The UK Extension to the EU-U.S. DPF reflects years of hard work, including in collaboration with you and your colleagues in the UK Government. We look forward to continuing to work with the UK Department of Science, Innovation and Technology ("DSIT") and the UK Information Commissioner's Office ("ICO")[1] to ensure that this collaborative effort functions effectively.

The UK Extension to the EU-U.S. DPF will yield significant benefits for both individuals and businesses. First, it provides an important set of privacy protections for the data of UK individuals transferred to the United States.[2] It requires participating U.S. organizations to develop a conforming privacy policy; in relation to personal data transferred from the European Union and the United Kingdom, publicly commit to comply with the "EU-U.S. Data Privacy Framework Principles", including the Supplemental Principles (collectively "the Principles"), and Annex I of the Principles (*i.e.*, an annex providing the terms under which EU-U.S. DPF

[1] References herein to the ICO should generally be understood as referring to the Gibraltar Regulatory Authority ("GRA") as relates to personal data received from Gibraltar in reliance on the UK Extension to the EU-U.S. DPF. For the purposes of the UK Extension to the EU-U.S. DPF, DSIT and the ICO will, as appropriate, facilitate cooperation between the Department and the GRA.

[2] Under the UK Extension to the EU-U.S. DPF the safeguards, protections, and administration and supervision of the EU-U.S. DPF will extend to personal data transfers from the United Kingdom and Gibraltar to U.S. organizations that elect to participate in the UK Extension to the EU-U.S. DPF. Such safeguards, protections, and administration and supervision, including relevant enforcement will apply to those personal data transfers from the United Kingdom and Gibraltar in a manner that is consistent with their application to personal data transfers from the European Union to U.S. organizations that participate in the EU-U.S. DPF.

organizations are obligated to arbitrate certain residual claims as to personal data covered by the Principles)[3], so that the commitment becomes enforceable under U.S. law[4]; annually re-certify their compliance to the Department; provide free, independent dispute resolution to UK individuals; and be subject to the investigatory and enforcement authority of a U.S. statutory body listed in the Principles (*e.g.*, the Federal Trade Commission (the "FTC") and Department of Transportation (the "DOT")), or a U.S. statutory body listed in a future annex to the Principles. While an organization's decision to self-certify is voluntary, once an organization publicly commits to comply with the Principles, including as relates to personal data received from the United Kingdom in reliance on the UK Extension to the EU-U.S. DPF, its commitment is enforceable under U.S. law by the FTC, DOT, or another U.S. statutory body depending on which body has jurisdiction over the participating organization.[5] Second, the UK Extension to the EU-U.S. DPF will enable businessess in the United States, including subsidiaries of European businesses located in the United States, to receive personal data from the United Kingdom to facilitate data flows that support transatlantic trade. Data flows between the United States and the United Kingdom underpin the $1.8 trillion U.S.-UK economic relationship, which supports millions of jobs on both sides of the Atlantic. Businesses that rely on transatlantic data flows come from all industry sectors and include major Fortune 500 firms, as well as many small and medium-sized enterprises. Transatlantic data flows allow U.S. organizations to process data required to offer goods, services, and employment opportunities to UK individuals.

The Department is committed to working closely and productively with our UK counterparts to effectively administer and supervise the Data Privacy Framework program. This commitment is reflected in the Department's development and continued refinement of a variety of resources to assist organizations with the self-certification process, creation of a website to provide targeted information to stakeholders, collaboration with DSIT and the ICO to develop

---

[3] Under the UK Extension to the EU-U.S. DPF personal data transfers from the United Kingdom and Gibraltar to the United States shall, as appropriate (*i.e.*, where the organization has elected to cover such transfers), be treated in accordance with the Principles and Annex I of the Principles. It follows that for the purposes of the UK Extension to the EU-U.S. DPF references in the Principles and Annex I of the Principles to the European Union and/or the European Commission, EU DPAs, and EU individuals should generally be understood as referring respectively to the United Kingdom and/or the UK Government, the ICO and/or, as applicable, the GRA, and UK individuals (*i.e.*, as consistent with relevant differences between the United Kingdom and Gibraltar, and the European Union).

[4] Organizations that self-certified their commitment to comply with the EU-U.S. Privacy Shield Framework Principles and wish to enjoy the benefits of participating in the EU-U.S. DPF must comply with the "EU-U.S. Data Privacy Framework Principles". This commitment to comply with the "EU-U.S. Data Privacy Framework Principles" shall be reflected in the privacy policies of such participating organizations as soon as possible, and in any event no later than three months from the effective date for the "EU-U.S. Data Privacy Framework Principles". (*See* section (e) of the Supplemental Principle on Self-Certification).

[5] Effective as of July 17, 2023 organizations that wish to self-certify their compliance pursuant to the UK Extension to the EU-U.S. DPF may do so; however, personal data cannot be received from the United Kingdom in reliance on the UK Extension to the EU-U.S. DPF before the date that the adequacy regulations implementing the data bridge for the UK Extension to the EU-U.S. DPF enter into force. Organizations that wish to receive personal data from the United Kingdom and Gibraltar in reliance on the UK Extension to the EU-U.S. DPF must comply with the Principles with regard to such data. This commitment to comply shall be reflected in such organizations' self-certification submissions to the Department, and in their privacy policies. An organization that already participates in the EU-U.S. DPF and intends to extend its participation to also cover personal data received from the United Kingdom and Gibraltar would make its election to participate in the UK Extension to the EU-U.S. DPF either: (a) as part of its annual re-certification to the EU-U.S. DPF, or (b) outside of its annual re-certification to the EU-U.S. DPF provided it makes that election no later than six months from July 17, 2023. An organization that does not already participate in the EU-U.S. DPF and intends for its participation to also cover personal data received from the United Kingdom and Gibraltar would make its election to participate in the UK Extension to the EU-U.S. DPF as part of its initial self-certification to the EU-U.S. DPF.

guidance that clarifies important elements of the UK Extension to the EU-U.S. DPF[6], outreach to facilitate increased understanding of organizations' data protection obligations, and oversight and monitoring of organizations' compliance with the program's requirements.

Our ongoing cooperation with valued UK counterparts will enable the Department to ensure that the UK Extension to the EU-U.S. DPF functions effectively. The United States Government has a long history of working with the UK Government to promote shared data protection principles while furthering trade and economic growth in the United Kingdom and the United States. We believe that the UK Extension to the EU-U.S. DPF, which is an example of this cooperation, will allow the United Kingdom to grant a data bridge to the United States thereby enabling organizations to transfer personal data from the United Kingdom to the United States consistent with UK law.

Administration and Supervision of the Data Privacy Framework Program by the Department of Commerce

The Department is firmly committed to the effective administration and supervision of the Data Privacy Framework program and will undertake appropriate efforts and dedicate appropriate resources to ensure that outcome.[7] The Department will maintain and make available to the public an authoritative list of U.S. organizations that have self-certified to the Department and declared their commitment to adhere to the Principles ("the Data Privacy Framework List"), which it will update on the basis of annual re-certification submissions made by participating organizations and by removing organizations when they voluntarily withdraw, fail to complete the annual re-certification in accordance with the Department's procedures, or are found to persistently fail to comply. The Department will also maintain and make available to the public an authoritative record of U.S. organizations that have been removed from the Data Privacy Framework List and will identify the reason each organization was removed. The aforementioned authoritative list and record will remain available to the public on the Department's Data Privacy Framework website.[8] The Data Privacy Framework website will include a prominently placed explanation indicating that any organization removed from the Data Privacy Framework List must cease making claims that it participates in or complies with the EU-U.S. DPF and/or UK Extension to the EU-U.S. DPF (as applicable) and that it may receive personal information pursuant to the EU-U.S. DPF and/or UK Extension to the EU-U.S. DPF (as applicable). Such an organization must nevertheless continue to apply the Principles to the personal information that it received while it participated in the EU-U.S. DPF and/or UK Extension to the EU-U.S. DPF (as applicable) for as long as it retains such information. The Department, in furtherance of its overarching, ongoing commitment to the effective administration and supervision of the Data Privacy Framework program, specifically undertakes to do the following:

Verify Self-Certification Requirements

---

[6] Guidance to assist organizations with the self-certification process as relates to electing to participate in the UK Extension to the EU-U.S. DPF, including guidance developed in collaboration with DSIT and the ICO to clarify important elements of the UK Extension to the EU-U.S. DPF, as well as targeted information for stakeholders will be made available on the Department's Data Privacy Framework website.

[7] Although the administration and supervision of the Data Privacy Framework program will be as consistent as possible for the UK Extension to the EU-U.S. DPF and the EU-U.S. DPF, such administration and supervision will reflect relevant differences between the United Kingdom and Gibraltar, and the European Union.

[8] That authoritative list (*i.e.*, the Data Privacy Framework List), as well as that authoritative record will respectively indicate whether the featured U.S. organizations participate or have participated in the UK Extension to the EU-U.S. DPF.

- The Department will, prior to finalizing an organization's initial self-certification or annual re-certification (collectively "self-certification"), including where the organization has elected to participate in the UK Extension to the EU-U.S. DPF, and then placing or maintaining the organization on the Data Privacy Framework List, verify that the organization has, at a minimum, met the relevant requirements set forth in the Supplemental Principle on Self-Certification concerning what information an organization must provide in its self-certification submission to the Department and provided at an appropriate time a relevant privacy policy that informs individuals about all 13 of the enumerated elements set forth in the Notice Principle. The Department will verify that the organization has:
    - identified the organization that is submitting its self-certification, as well as any U.S. entities or U.S. subsidiaries of the self-certifying organization that are also adhering to the Principles that the organization wishes to be covered by its self-certification;
    - provided required organization contact information (*e.g.*, contact information for specific individual(s) and/or office(s) within the self-certifying organization responsible for handling complaints, access requests, and any other issues arising under the EU-U.S. DPF and/or UK Extension to the EU-U.S. DPF (as applicable));
    - described the purpose(s) for which the organization would collect and use personal information received from the European Union and the United Kingdom;
    - indicated what personal information would be received from the European Union in reliance on the EU-U.S. DPF and the United Kingdom in reliance on the UK Extension to the EU-U.S. DPF and therefore be covered by its self-certification;
    - if the organization has a public website, provided the web address where the relevant privacy policy is readily available on that website, or if the organization does not have a public website, provided the Department with a copy of the relevant privacy policy and where that privacy policy is available for viewing by affected individuals (*i.e.*, affected employees if the relevant privacy policy is a human resources privacy policy or the public if the relevant privacy policy is not a human resources privacy policy);
    - included in its relevant privacy policy at the appropriate time (*i.e.*, initially only in a draft privacy policy provided along with the submission if that submission is an initial self-certification; otherwise, in a final and where applicable published privacy policy) a statement that it adheres to the Principles, including as relates to personal data received from the United Kingdom in reliance on the UK Extension to the EU-U.S. DPF and a hyperlink to or the web address for the Department's Data Privacy Framework website (*e.g.*, the homepage or the Data Privacy Framework List web page);
    - included in its relevant privacy policy at the appropriate time all of the 12 other enumerated elements set forth in the Notice Principle (*e.g.*, the possibility, under certain conditions, for the affected EU or UK individual to invoke binding arbitration[9]; the requirement to disclose personal information in response to lawful requests by public authorities, including to meet national security or law enforcement requirements; and its liability in cases of onward transfers to third parties);
    - identified the specific statutory body that has jurisdiction to hear any claims against the organization regarding possible unfair or deceptive practices and violations of

[9] Under the UK Extension to the EU-U.S. DPF the provisions of the Principles and Annex I of the Principles concerning the possibility, under certain circumstances, for individuals to invoke binding arbitration, including those provisions that describe organizations' obligations to arbitrate claims and follow the terms set forth in Annex I of the Principles will apply, as appropriate, to personal data transfers from the United Kingdom and Gibraltar to the United States in a manner that is consistent with that applied to personal data transfers from the European Union to the United States.

laws or regulations governing privacy (and that is listed in the Principles or a future annex to the Principles);
    - identified any privacy program in which the organization is a member;
    - identified whether the relevant method (*i.e.*, follow-up procedures that it must provide) for verifying its compliance with the Principles is "self-assessment" (*i.e.*, in-house verification) or "outside compliance review" (*i.e.*, third-party verification) and if it identified the relevant method as outside compliance review, also identified the third party that has completed that review;
    - identified the appropriate independent recourse mechanism that is available to address complaints brought under the Principles and provide appropriate recourse free of charge to the affected individual.
        - If the organization has selected an independent recourse mechanism provided by a private-sector alternative dispute resolution body, it included in its relevant privacy policy a hyperlink to or the web address for the relevant website or complaint submission form of the mechanism that is available to investigate unresolved complaints brought under the Principles.[10]
        - If the organization either is required to (*i.e.*, with respect to human resources data transferred from the European Union and/or the United Kingdom in the context of the employment relationship) or has elected to cooperate with the appropriate EU data protection authorities ("DPAs") and/or ICO (as applicable) in the investigation and resolution of complaints brought under the Principles, it declared its commitment to such cooperation with the EU DPAs and/or ICO (as applicable) and compliance with their/its related advice to take specific action to comply with the Principles.[11]
- The Department will also verify that the organization's self-certification submission is consistent with its relevant privacy policy/ies. Where a self-certifying organization wishes to cover any of its U.S. entities or U.S. subsidiaries that have separate, relevant privacy policies, the Department will also review the relevant privacy policies of such covered entities or subsidiaries to ensure that they include all of the required elements set forth in the Notice Principle.
- The Department will work with statutory bodies (*e.g.*, FTC and DOT) to verify that the organizations are subject to the jurisdiction of the relevant statutory body identified in their self-certification submissions, where the Department has reason to doubt that they are subject to that jurisdiction.
- The Department will work with private-sector alternative dispute resolution bodies to verify that the organizations are actively registered for the independent recourse mechanism identified in their self-certification submissions; and work with those bodies to verify that the organizations are actively registered for the outside compliance review identified in their self-certification submissions, where those bodies may offer both types of services.

---

[10] Under the UK Extension to the EU-U.S. DPF the provisions of the Principles and Annex I of the Principles concerning independent recourse mechanisms, including those that describe organizations' obligations with regard to such mechanisms and the obligations applicable to the mechanisms themselves, will apply, as appropriate, to personal data transfers from the United Kingdom and Gibraltar to the United States in a manner that is consistent with that applied to personal data transfers from the European Union to the United States.

[11] Under the UK Extension to the EU-U.S. DPF the provisions of the Principles and Annex I of the Principles concerning the EU DPAs, including those provisions that describe organizations' obligations to cooperate with the EU DPAs and comply with their related advice to take specific action to comply with the Principles will apply, as appropriate, to personal data transfers from the United Kingdom and Gibraltar to the United States in a manner that is consistent with that applied to personal data transfers from the European Union to the United States (*i.e.*, such provisions of the Principles should generally be understood as referring to organizations' obligations to cooperate with and comply with the advice of the ICO and/or, as applicable, the GRA).

- The Department will work with the third party selected by the Department to administer arbitrations pursuant to and manage the arbitral fund identified in Annex I of the Principles to verify that the organizations have contributed to that arbitral fund.
- Where the Department identifies any issues during its review of organizations' self-certification submissions, it will inform them that they must address all such issues within the appropriate timeframe designated by the Department.[12] The Department will also inform them that failure to respond within timeframes designated by the Department or other failure to complete their self-certification in accordance with the Department's procedures will lead to those self-certification submissions being considered abandoned, and that any misrepresentation about an organization's participation in or compliance with the EU-U.S. DPF may be subject to enforcement action by the FTC, the DOT, or other relevant government body. The Department will inform the organizations through the means of contact that the organizations provided to the Department.

Facilitate Cooperation with Alternative Dispute Resolution Bodies That Provide Principles-Related Services

- The Department will work with private-sector alternative dispute resolution bodies providing independent recourse mechanisms, which are available to investigate unresolved complaints brought under the Principles, to verify that they meet, at a minimum, the requirements set forth in the Supplemental Principle on Dispute Resolution and Enforcement. The Department will verify that they:
    - include information on their public websites regarding the Principles and the services that they provide under the EU-U.S. DPF and/or UK Extension to the EU-U.S. DPF (as applicable), which must include: (1) information on or a hyperlink to the Principles' requirements for independent recourse mechanisms; (2) a hyperlink to the Department's Data Privacy Framework website; (3) an explanation that their dispute resolution services under the EU-U.S. DPF and/or UK Extension to the EU-U.S. DPF (as applicable) are free of charge to individuals; (4) a description of how a Principles-related complaint can be filed; (5) the timeframe in which Principles-related complaints are processed; and (6) a description of the range of potential remedies. The Department will provide the bodies with timely notice of material changes to the Department's supervision and administration of the Data Privacy Framework program, where such changes are imminent or have already been made and such changes are relevant to the role that the bodies play under the EU-U.S. DPF and/or UK Extension to the EU-U.S. DPF (as applicable);
    - publish an annual report providing aggregate statistics regarding their dispute resolution services, which must include: (1) the total number of Principles-related complaints received during the reporting year; (2) the types of complaints received; (3) dispute resolution quality measures, such as the length of time taken to process complaints; and (4) the outcomes of the complaints received, notably the number and types of remedies or sanctions imposed. The Department will provide the bodies with specific, complementary guidance on what information they should provide in those annual reports elaborating upon those requirements (*e.g.*, listing the specific criteria that a complaint must meet to be considered a Principles-related complaint for purposes of the annual report), as well as identifying other types of information they should provide (*e.g.*, if the body also provides a Principles-related verification service, a description of how the body avoids any actual or potential conflicts of

[12] *E.g.*, As regards re-certification, the expectation would be that organizations address all such issues within 45 days; subject to the designation by the Department of a different, appropriate timeframe.

interest in situations when it provides an organization with both verification services and dispute resolution services). The additional guidance provided by the Department will also specify the date by which the bodies' annual reports should be published for the relevant reporting period.

Follow Up with Organizations That Wish to Be or Have Been Removed from the Data Privacy Framework List

- If an organization that participates in the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF wishes to withdraw from the EU-U.S. DPF, such withdrawal would necessarily include withdrawal from the UK Extension to the EU-U.S. DPF and the Department will require that the organization remove from any relevant privacy policy any references to either the EU-U.S. DPF or UK Extension to the EU-U.S. DPF that imply that it continues to participate in the EU-U.S. DPF and that it may receive personal data pursuant to either the EU-U.S. DPF or UK Extension to the EU-U.S. DPF (*see* description of the Department's commitment to search for false claims of participation). If an organization exclusively wishes to withdraw from the UK Extension to the EU-U.S. DPF, the Department will require that the organization remove from any relevant privacy policy any references that imply that it continues to participate in the UK Extension to the EU-U.S. DPF and that it may receive personal data pursuant to the UK Extension to the EU-U.S. DPF. The Department will also require that the organization complete and submit to the Department an appropriate questionnaire to verify:
    - its wish to withdraw;
    - which of the following it will do with the personal data that it received in reliance on the EU-U.S. DPF and/or UK Extension to the EU-U.S. DPF (as applicable) while it participated in the EU-U.S. DPF and/or UK Extension to the EU-U.S. DPF (as applicable): (a) retain such data, continue to apply the Principles to such data, and affirm to the Department on an annual basis its commitment to apply the Principles to such data; (b) retain such data and provide "adequate" protection for such data by another authorized means; or (c) return or delete all such data by a specified date; and
    - who within the organization will serve as an ongoing point of contact for Principles-related questions.
- If an organization elected (a) as described immediately above, the Department will also require that it complete and submit to the Department each year after its withdrawal (*i.e.,* by the first anniversary of its withdrawal, as well as by every subsequent anniversary unless and until the organization either provides "adequate" protection for such data by another authorized means or returns or deletes all such data and notifies the Department of this action) an appropriate questionnaire to verify what it has done with that personal data, what it will do with any of that personal data that it continues to retain, and who within the organization will serve as an ongoing point of contact for Principles-related questions.
- If an organization has allowed its self-certification to lapse (*i.e.*, neither completed its annual re-certification of its adherence to the Principles nor was removed from the Data Privacy Framework List for some other reason, such as withdrawal), the Department will direct it to complete and submit to the Department an appropriate questionnaire to verify whether it wishes to withdraw or re-certify:
    - and if it wishes to withdraw, further verify what it will do with the personal data that it received in reliance on the EU-U.S. DPF and/or UK Extension to the EU-U.S. DPF (as applicable) while it participated in the EU-U.S. DPF and/or UK Extension to the

EU-U.S. DPF (as applicable) (*see* previous description of what an organization must verify if it wishes to withdraw);
    - and if it intends to re-certify, further verify that during the lapse of its certification status it applied the Principles to personal data received under the EU-U.S. DPF and/or UK Extension to the EU-U.S. DPF (as applicable) and clarify what steps it will take to address the outstanding issues that have delayed its re-certification.
- If an organization is removed from the Data Privacy Framework List for any of the following reasons: (a) withdrawal from the EU-U.S. DPF and/or UK Extension to the EU-U.S. DPF (as applicable), (b) failure to complete the annual re-certification of its adherence to the Principles (*i.e.*, either started, but failed to complete the annual re-certification process in a timely manner or did not even start the annual re-certification process), or (c) "persistent failure to comply", the Department will send a notification to the contact(s) identified in the organization's self-certification submission specifying the reason for the removal and explaining that it must cease making any explicit or implicit claims that it participates in or complies with the EU-U.S. DPF and/or UK Extension to the EU-U.S. DPF (as applicable) and that it may receive personal data pursuant to the EU-U.S. DPF and/or UK Extension to the EU-U.S. DPF (as applicable). The notification, which may also include other content tailored to fit the reason for the removal, will indicate that organizations misrepresenting their participation in or compliance with the EU-U.S. DPF and/or UK Extension to the EU-U.S. DPF (as applicable), including where they represent that they are participating in the EU-U.S. DPF and/or UK Extension to the EU-U.S. DPF (as applicable) after having been removed from the Data Privacy Framework List, may be subject to enforcement action by the FTC, the DOT, or other relevant government body.

Search for and Address False Claims of Participation

- On an ongoing basis, when an organization: (a) withdraws from participation in the EU-U.S. DPF and/or UK Extension to the EU-U.S. DPF (as applicable), (b) fails to complete the annual re-certification of its adherence to the Principles (*i.e.*, either started, but failed to complete the annual re-certification process in a timely manner or did not even start the annual re-certification process), (c) is removed as a participant in the EU-U.S. DPF and/or UK Extension to the EU-U.S. DPF (as applicable) notably for "persistent failure to comply," or (d) fails to complete an initial self-certification of its adherence to the Principles (*i.e.*, started, but failed to complete the initial self-certification process in a timely manner), the Department will undertake, on an *ex officio* basis action to verify that any relevant published privacy policy of the organization does not contain references to the EU-U.S. DPF and/or UK Extension to the EU-U.S. DPF (as applicable) that imply that the organization participates in the EU-U.S. DPF and/or UK Extension to the EU-U.S. DPF (as applicable) and that it may receive personal data pursuant to the EU-U.S. DPF and/or UK Extension to the EU-U.S. DPF (as applicable). Where the Department finds such references, the Department will inform the organization that the Department will, as appropriate, refer the matter to the relevant agency for potential enforcement action if the organization continues to misrepresent its participation in the EU-U.S. DPF and/or UK Extension to the EU-U.S. DPF (as applicable). The Department will inform the organization through the means of contact the organization provided to the Department or where necessary other appropriate means. If the organization neither removes the references nor self-certifies its compliance under the EU-U.S. DPF and/or UK Extension to the EU-U.S. DPF (as applicable) in accordance with the Department's procedures, the Department will *ex officio*, refer the matter to the FTC, DOT, or other appropriate enforcement agency, or take other appropriate action to ensure proper use of the EU-U.S. DPF certification mark;

- The Department will undertake other efforts to identify false claims of EU-U.S. DPF and/or UK Extension to the EU-U.S. DPF (as applicable) participation and improper use of the EU-U.S. DPF certification mark, including by organizations that unlike the organizations described immediately above have never even started the self-certification process (*e.g.*, conducting appropriate Internet searches to identify references to the EU-U.S. DPF and/or UK Extension to the EU-U.S. DPF (as applicable) in organizations' privacy policies). Where through such efforts the Department identifies false claims of EU-U.S. DPF and/or UK Extension to the EU-U.S. DPF (as applicable) participation and improper use of the EU-U.S. DPF certification mark, the Department will inform the organization that the Department will, as appropriate, refer the matter to the relevant agency for potential enforcement action if the organization continues to misrepresent its participation in the EU-U.S. DPF and/or UK Extension to the EU-U.S. DPF (as applicable). The Department will inform the organization through the means of contact, if any, the organization provided to the Department or where necessary other appropriate means. If the organization neither removes the references nor self-certifies its compliance under the EU-U.S. DPF and/or UK Extension to the EU-U.S. DPF (as applicable) in accordance with the Department's procedures, the Department will *ex officio*, refer the matter to the FTC, DOT, or other appropriate enforcement agency, or take other appropriate action to ensure proper use of the EU-U.S. DPF certification mark;
- The Department will promptly review and address specific, non-frivolous complaints about false claims of EU-U.S. DPF and/or UK Extension to the EU-U.S. DPF (as applicable) participation that the Department receives (*e.g.*, complaints received from the EU DPAs and/or ICO, independent recourse mechanisms provided by private-sector alternative dispute resolution bodies, data subjects, EU, UK, and U.S. businesses, and other types of third parties); and
- The Department may take other appropriate corrective action. Misrepresentations to the Department may be actionable under the False Statements Act (18 U.S.C. § 1001).

Conduct Periodic *ex officio* Compliance Reviews and Assessments of the Data Privacy Framework Program

- On an ongoing basis, the Department will undertake efforts to monitor effective compliance by EU-U.S. DPF and/or UK Extension to the EU-U.S. DPF (as applicable) organizations to identify issues that may warrant follow-up action. In particular, the Department will conduct, on an *ex officio* basis routine spot checks of randomly selected EU-U.S. DPF and/or UK Extension to the EU-U.S. DPF (as applicable) organizations, as well as *ad hoc* spot checks of specific EU-U.S. DPF and/or UK Extension to the EU-U.S. DPF (as applicable) organizations when potential compliance deficiencies are identified (*e.g.*, potential compliance deficiencies brought to the attention of the Department by third parties) to verify: (a) that the point(s) of contact responsible for the handling of complaints, access requests, and other issues arising under the EU-U.S. DPF and/or UK Extension to the EU-U.S. DPF (as applicable) are available; (b) where applicable, that the organization's public-facing privacy policy is readily available for viewing by the public both on the organization's public website and via a hyperlink on the Data Privacy Framework List; (c) that the organization's privacy policy continues to comply with the self-certification requirements described in the Principles; and (d) that the independent recourse mechanism identified by the organization is available to address complaints brought under the EU-U.S. DPF and/or UK Extension to the EU-U.S. DPF (as applicable). The Department will also actively monitor the news for reports that provide credible evidence of non-compliance by EU-U.S. DPF and UK Extension to the EU-U.S. DPF organizations;

- As part of the compliance review, the Department will require that a EU-U.S. DPF and/or UK Extension to the EU-U.S. DPF (as applicable) organization complete and submit to the Department a detailed questionnaire when: (a) the Department has received any specific, non-frivolous complaints about the organization's compliance with the Principles, (b) the organization does not respond satisfactorily to inquiries by the Department for information relating to the EU-U.S. DPF and/or UK Extension to the EU-U.S. DPF (as applicable), or (c) there is credible evidence that the organization does not comply with its commitments under the EU-U.S. DPF and/or UK Extension to the EU-U.S. DPF (as applicable). Where the Department has sent such a detailed questionnaire to an organization and the organization fails to satisfactorily reply to the questionnaire, the Department will inform the organization that the Department will, as appropriate, refer the matter to the relevant agency for potential enforcement action if the Department does not receive a timely and satisfactory response from the organization. The Department will inform the organization through the means of contact the organization provided to the Department or where necessary other appropriate means. If the organization does not provide a timely and satisfactory response, the Department will *ex officio* refer the matter to the FTC, DOT, or other appropriate enforcement agency, or take other appropriate action towards ensuring compliance. The Department shall, when appropriate, consult with the competent data protection authority/ies (*e.g.*, the ICO) about such compliance reviews; and
- The Department will assess periodically the administration and supervision of the Data Privacy Framework program to ensure that its monitoring efforts, including any such efforts undertaken through the use of search tools (*e.g.*, to check for broken links to EU-U.S. DPF and/or UK Extension to the EU-U.S. DPF (as applicable) organizations' privacy policies), are appropriate to address existing issues and any new issues as they arise.

Tailor the Data Privacy Framework Website to Targeted Audiences

The Department will tailor the Data Privacy Framework website to focus on the following target audiences: UK individuals, UK businesses, U.S. businesses, and the ICO. The inclusion of material targeted directly to UK individuals and UK businesses will facilitate transparency in a number of ways. With regard to UK individuals, the website will clearly explain: (1) the rights the UK Extension to the EU-U.S. DPF provides to UK individuals; (2) the recourse mechanisms available to UK individuals when they believe an organization has breached its commitment to comply with the Principles; and (3) how to find information pertaining to an organization's self-certification, including as relates to its election to participate in the UK Extension to the EU-U.S. DPF. With regard to UK businesses, it will facilitate verification of: (1) whether an organization is a participant in the UK Extension to the EU-U.S. DPF; (2) the type of information covered by an organization's self-certification, including any received in reliance on the UK Extension to the EU-U.S. DPF; (3) the privacy policy that applies to the covered information; and (4) the method the organization uses to verify its adherence to the Principles. With regard to U.S. businesses, it will clearly explain: (1) the benefits of EU-U.S. DPF participation, including as relates to the UK Extension to the EU-U.S. DPF; (2) how to elect to participate in the UK Extension to the EU-U.S. DPF, re-certify to the EU-U.S. DPF and UK Extension to the EU-U.S. DPF, and withdraw from the UK Extension to the EU-U.S. DPF; and (3) how the United States administers and enforces the UK Extension to the EU-U.S. DPF. The inclusion of material targeted directly to the ICO (*e.g.*, information about the Department's dedicated point of contact for the ICO and a hyperlink to Principles-related content on the FTC website) will facilitate both cooperation and transparency. The Department will also work on an *ad hoc* basis with DSIT and the ICO to develop additional, topical material (*e.g.*, answers to frequently asked questions) for use on the Data Privacy Framework website, where such

information would facilitate the efficient administration and supervision of the Data Privacy Framework program.

Facilitate Cooperation with the ICO

To increase opportunities for cooperation with the ICO, the Department will maintain a dedicated point of contact at the Department to act as a liaison with the ICO. In instances where the ICO believes that a UK Extension to the EU-U.S. DPF organization is not complying with the Principles, including following a complaint from a UK individual, the ICO will be able to reach out to the dedicated point of contact at the Department to refer the organization for further review. The Department will make its best effort to facilitate resolution of the complaint with the UK Extension to the EU-U.S. DPF organization. Within 90 days after receipt of the complaint, the Department will provide an update to the ICO. The dedicated point of contact will also receive referrals regarding organizations that falsely claim to participate in the UK Extension to the EU-U.S. DPF. The dedicated point of contact will track all referrals from the ICO received by the Department, and the Department will provide pursuant to the data bridge dialogue described below a report analyzing in aggregate the complaints it receives each year. The dedicated point of contact will assist the ICO when it seeks information related to a specific organization's self-certification or previous participation in the UK Extension to the EU-U.S. DPF, and the dedicated point of contact will respond to the ICO's inquiries regarding the implementation of specific UK Extension to the EU-U.S. DPF requirements. In addition, the Department will provide the ICO with material regarding the UK Extension to the EU-U.S. DPF for inclusion on its own website to increase transparency for UK individuals and UK businesses. Increased awareness regarding the UK Extension to the EU-U.S. DPF and the rights and responsibilities it creates should facilitate the identification of issues as they arise, so that these can be appropriately addressed.

Fulfill Its Commitments under Annex I of the Principles

The Department will fulfill its commitments under Annex I of the Principles, including maintaining a list of arbitrators chosen with the European Commission on the basis of independence, integrity, and expertise; and supporting, as appropriate, the third party selected by the Department to administer arbitrations pursuant to and manage the arbitral fund identified in Annex I of the Principles.[13] The Department will work with the third party to, among other things, verify that the third party maintains a website with guidance on the arbitration process, including: (1) how to initiate proceedings and submit documents; (2) the list of arbitrators maintained by the Department and how to select arbitrators from that list; (3) the governing arbitral procedures and arbitrator code of conduct adopted by the Department and the European Commission;[14] and (4) the collection and payment of arbitrator fees.[15] In addition, the

[13] The International Centre for Dispute Resolution ("ICDR"), the international division of the American Arbitration Association ("AAA") (collectively "ICDR-AAA"), was selected by the Department to administer arbitrations pursuant to and manage the arbitral fund identified in Annex I of the Principles.

[14] On September 15, 2017, the Department and the European Commission agreed to the adoption of a set of arbitral rules to govern binding arbitration proceedings described in Annex I of the Principles, as well as a code of conduct for arbitrators that is consistent with generally accepted ethical standards for commercial arbitrators and Annex I of the Principles. The Department and the European Commission agreed to adapt the arbitration rules and code of conduct to reflect the updates under the EU-U.S. DPF, and the Department will work with the ICDR-AAA to make those updates.

[15] The Department will work with the ICDR-AAA, as appropriate, in developing relevant guidance on the arbitration process, including as relates to the UK Extension to the EU-U.S. DPF, for use on the website maintained by the ICDR-AAA.

Department will work with the third party to periodically review the operation of the arbitral fund, including the need to adjust the amount of the contributions or the caps (*i.e.*, maximum amounts) on the arbitral cost, and consider, among other things, the number of arbitrations and the costs and timing of the arbitrations, with the understanding that there will be no excessive financial burden imposed on EU-U.S. DPF and/or UK Extension to the EU-U.S. DPF (as applicable) organizations. The Department will notify the European Commission of the outcome of such reviews with the third party and will provide the European Commission with prior notification of any adjustments of the amount of the contributions.[16]

Participate in Discussions under the UK-U.S. Data Bridge Dialogue

The Department and other agencies, as appropriate, will hold discussions on a periodic basis with DSIT, and the ICO, as appropriate, where the Department will provide updates on the UK Extension to the EU-U.S. DPF. The discussions will include consideration of current issues related to the functioning, implementation, supervision, and enforcement of the Data Privacy Framework program. The discussions may, as appropriate, include consideration of related topics, such as other data transfer mechanisms that benefit from the safeguards under the UK Extension to the EU-U.S. DPF.

Update of Laws

The Department will make reasonable efforts to inform DSIT of material developments in the law in the United States so far as they are relevant to the UK Extension to the EU-U.S. DPF in the field of data privacy protection and the limitations and safeguards applicable to access to personal data by U.S. authorities and its subsequent use.

U.S. Government Access to Personal Data

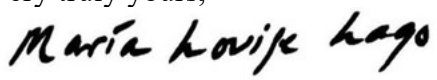
The United States has issued Executive Order 14086, "Enhancing Safeguards for United States Signals Intelligence Activities" and 28 CFR part 201 amending Department of Justice regulations to establish the Data Protection Review Court (the "DPRC"), which provide strong protection for personal data with respect to government access to data for national security purposes. The protection provided includes: strengthening privacy and civil liberties safeguards to ensure that U.S. signals intelligence activities are necessary and proportionate in the pursuit of defined national security objectives; establishing a new redress mechanism with independent and binding authority; and enhancing the existing rigorous and layered oversight of U.S. signals intelligence activities. Through these protections, UK individuals may seek redress from a new multi-layer redress mechanism that includes an independent DPRC that would consist of individuals chosen from outside the U.S. Government who would have full authority to adjudicate claims and direct remedial measures as needed. The Department will maintain a record of UK individuals who submit a qualifying complaint pursuant to Executive Order 14086 and 28 CFR part 201. Five years after the date of this letter, and on a five-year basis thereafter, the Department will contact relevant agencies regarding whether information pertaining to the review of qualifying complaints or review of any applications for review submitted to the DPRC has been declassified. If such information has been declassified, the Department will work with the ICO to inform the UK individual. These enhancements confirm that UK personal data

[16] The Department will provide DSIT with timely notice of the outcome of such reviews with the third party, as well as any adjustments of the amount of the contributions (*e.g.*, such issues could be considered, along with other issues related to the functioning, implementation, supervision, and enforcement of the Data Privacy Framework program as part of the discussions under the data bridge dialogue described above).

transferred to the United States will be treated in a manner consistent with UK legal requirements with respect to government access to data.

On the basis of the Principles, Executive Order 14086, 28 CFR part 201, and the accompanying letters and materials, including the Department's commitments regarding the administration and supervision of the Data Privacy Framework program, our expectation is that the UK Secretary of State for Science, Innovation and Technology will determine that the UK Extension to the EU-U.S. DPF provides adequate protection for the purposes of UK law and data transfers from the United Kingdom and Gibraltar will continue to organizations that participate in the UK Extension to the EU-U.S. DPF. We also expect that those arrangements will further facilitate transfers to U.S. organizations made in reliance on other data transfer mechanisms under UK law, including UK International Data Transfer Agreements or UK Binding Corporate Rules.

Very truly yours,



Marisa Lago
Under Secretary for International Trade