

EU-U.S. DATA PRIVACY FRAMEWORK PRINCIPLES ISSUED BY THE U.S. DEPARTMENT OF COMMERCE

I. OVERVIEW

1. While the United States and the European Union (the “EU”) share a commitment to enhancing privacy protection, the rule of law, and a recognition of the importance of transatlantic data flows to our respective citizens, economies, and societies, the United States takes a different approach to privacy protection from that taken by the EU. The United States uses a sectoral approach that relies on a mix of legislation, regulation, and self-regulation. The U.S. Department of Commerce (“the Department”) is issuing the EU-U.S. Data Privacy Framework Principles, including the Supplemental Principles (collectively “the Principles”) and Annex I of the Principles (“Annex I”), under its statutory authority to foster, promote, and develop international commerce (15 U.S.C. § 1512). The Principles were developed in consultation with the European Commission (“the Commission”), industry, and other stakeholders to facilitate trade and commerce between the United States and EU. The Principles, a key component of the EU-U.S. Data Privacy Framework (“EU-U.S. DPF”), provide organizations in the United States with a reliable mechanism for personal data transfers to the United States from the EU while ensuring that EU data subjects continue to benefit from effective safeguards and protection as required by European legislation with respect to the processing of their personal data when they have been transferred to non-EU countries. The Principles are intended for use solely by eligible organizations in the United States receiving personal data from the EU for the purpose of qualifying for the EU-U.S. DPF and thus benefitting from the Commission’s adequacy decision.¹ The Principles do not affect the application of the Regulation (EU) 2016/679 (“the General Data Protection Regulation” or “the GDPR”)² that applies to the processing of personal data in the EU Member States. Nor do the Principles limit privacy obligations that otherwise apply under U.S. law.

2. In order to rely on the EU-U.S. DPF to effectuate transfers of personal data from the EU, an organization must self-certify its adherence to the Principles to the Department (or its designee). While decisions by organizations to thus enter the EU-U.S. DPF are entirely voluntary, effective compliance is compulsory: organizations that self-certify to the Department and publicly declare their commitment to adhere to the Principles must comply fully with the Principles. In order to enter the EU-U.S. DPF, an organization must (a) be subject to the investigatory and enforcement powers of the Federal Trade Commission (the “FTC”), the U.S. Department of Transportation (the “DOT”) or another

¹ Provided that the Commission Decision on the adequacy of the protection provided by the EU-U.S. DPF applies to Iceland, Liechtenstein and Norway, the EU-U.S. DPF will cover both the EU, as well as these three countries. Consequently, references to the EU and its Member States will be read as including Iceland, Liechtenstein, and Norway.

² REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

statutory body that will effectively ensure compliance with the Principles (*other U.S. statutory bodies recognized by the EU may be included as an annex in the future*); (b) publicly declare its commitment to comply with the Principles; (c) publicly disclose its privacy policies in line with these Principles; and (d) fully implement them³. An organization's failure to comply is enforceable by the FTC under Section 5 of the Federal Trade Commission (FTC) Act prohibiting unfair or deceptive acts in or affecting commerce (15 U.S.C. § 45); by the DOT under 49 U.S.C. § 41712 prohibiting a carrier or ticket agent from engaging in an unfair or deceptive practice in air transportation or the sale of air transportation; or under other laws or regulations prohibiting such acts.

3. 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"). EU-U.S. DPF benefits are assured from the date that the Department places the organization on the Data Privacy Framework List. The Department will remove from the Data Privacy Framework List those organizations that voluntarily withdraw from the EU-U.S. DPF or fail to complete their annual recertification to the Department; these organizations must either continue to apply the Principles to the personal information they received under the EU-U.S. DPF and affirm to the Department on an annual basis their commitment to do so (*i.e.*, for as long as they retain such information), provide "adequate" protection for the information by another authorized means (for example, using a contract that fully reflects the requirements of the relevant standard contractual clauses adopted by the Commission), or return or delete the information. The Department will also remove from the Data Privacy Framework List those organizations that have persistently failed to comply with the Principles; these organizations must return or delete the personal information they received under the EU-U.S. DPF. An organization's removal from the Data Privacy Framework List means it is no longer entitled to benefit from the Commission's adequacy decision to receive personal information from the EU.
4. The Department will also maintain and make available to the public an authoritative record of U.S. organizations that had previously self-certified to the Department, but that have been removed from the Data Privacy Framework List. The Department will provide a clear warning that these organizations are not participants in the EU-U.S. DPF; that removal from the Data Privacy Framework List means that such organizations cannot claim to be EU-U.S. DPF compliant and must avoid any statements or misleading practices implying that they participate in the EU-U.S. DPF; and that such organizations are no longer entitled to benefit from the Commission's adequacy decision to receive personal information from the EU. An organization that continues to claim participation in the EU-U.S. DPF or makes other EU-U.S. DPF-related misrepresentations after it has been removed from the Data Privacy Framework List may be subject to enforcement action by the FTC, the DOT, or other enforcement authorities.
5. Adherence to these Principles may be limited: (a) to the extent necessary to comply with a court order or meet public interest, law enforcement, or national

³ The EU-U.S. Privacy Shield Framework Principles have been amended as the "EU-U.S. Data Privacy Framework Principles". (*See* Supplemental Principle on Self-Certification).

security requirements, including where statute or government regulation create conflicting obligations; (b) by statute, court order, or government regulation that creates explicit authorizations, provided that, in exercising any such authorization, an organization can demonstrate that its non-compliance with the Principles is limited to the extent necessary to meet the overriding legitimate interests furthered by such authorization; or (c) if the effect of the GDPR is to allow exceptions or derogations, under the conditions set out therein, provided such exceptions or derogations are applied in comparable contexts. In this context, safeguards in U.S. law to protect privacy and civil liberties include those required by Executive Order 14086⁴ under the conditions set out therein (including its requirements on necessity and proportionality). Consistent with the goal of enhancing privacy protection, organizations should strive to implement these Principles fully and transparently, including by endeavouring to indicate in their privacy policies where exceptions to the Principles permitted by (b) above will apply. For the same reason, where the option is allowable under the Principles and/or U.S. law, organizations are expected to opt for the higher protection where possible.

6. Organizations are obligated to apply the Principles to all personal data transferred in reliance on the EU-U.S. DPF after they enter the EU-U.S. DPF. An organization that chooses to extend EU-U.S. DPF benefits to human resources personal information transferred from the EU for use in the context of an employment relationship must indicate this when it self-certifies to the Department and conform to the requirements set forth in the Supplemental Principle on Self-Certification.
7. U.S. law will apply to questions of interpretation and compliance with the Principles and relevant privacy policies by organizations participating in the EU-U.S. DPF, except where such organizations have committed to cooperate with EU data protection authorities (“DPAs”). Unless otherwise stated, all provisions of the Principles apply where they are relevant.
8. Definitions:
 - a. “Personal data” and “personal information” are data about an identified or identifiable individual that are within the scope of the GDPR, received by an organization in the United States from the EU, and recorded in any form.
 - b. “Processing” of personal data means any operation or set of operations which is performed upon personal data, whether or not by automated means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure or dissemination, and erasure or destruction.
 - c. “Controller” means a person or organization which, alone or jointly with others, determines the purposes and means of the processing of personal data.

⁴ Executive Order of October 7, 2022, "Enhancing Safeguards for United States Signals Intelligence Activities."

9. The effective date of the Principles and Annex I of the Principles is the date of entry into force of the European Commission's adequacy decision.

II. PRINCIPLES

1. NOTICE

- a. An organization must inform individuals about:
 - i. its participation in the EU-U.S. DPF and provide a link to, or the web address for, the Data Privacy Framework List,
 - ii. the types of personal data collected and, where applicable, the U.S. entities or U.S. subsidiaries of the organization also adhering to the Principles,
 - iii. its commitment to subject to the Principles all personal data received from the EU in reliance on the EU-U.S. DPF,
 - iv. the purposes for which it collects and uses personal information about them,
 - v. how to contact the organization with any inquiries or complaints, including any relevant establishment in the EU that can respond to such inquiries or complaints,
 - vi. the type or identity of third parties to which it discloses personal information, and the purposes for which it does so,
 - vii. the right of individuals to access their personal data,
 - viii. the choices and means the organization offers individuals for limiting the use and disclosure of their personal data,
 - ix. the independent dispute resolution body designated to address complaints and provide appropriate recourse free of charge to the individual, and whether it is: (1) the panel established by DPAs, (2) an alternative dispute resolution provider based in the EU, or (3) an alternative dispute resolution provider based in the United States,
 - x. being subject to the investigatory and enforcement powers of the FTC, the DOT or any other U.S. authorized statutory body,
 - xi. the possibility, under certain conditions, for the individual to invoke binding arbitration,⁵

⁵ See, e.g., section (c) of the Recourse, Enforcement and Liability Principle.

- xii. the requirement to disclose personal information in response to lawful requests by public authorities, including to meet national security or law enforcement requirements, and
 - xiii. its liability in cases of onward transfers to third parties.
- b. This notice must be provided in clear and conspicuous language when individuals are first asked to provide personal information to the organization or as soon thereafter as is practicable, but in any event before the organization uses such information for a purpose other than that for which it was originally collected or processed by the transferring organization or discloses it for the first time to a third party.

2. CHOICE

- a. An organization must offer individuals the opportunity to choose (*i.e.*, opt out) whether their personal information is (i) to be disclosed to a third party or (ii) to be used for a purpose that is materially different from the purpose(s) for which it was originally collected or subsequently authorized by the individuals. Individuals must be provided with clear, conspicuous, and readily available mechanisms to exercise choice.
- b. By derogation to the previous paragraph, it is not necessary to provide choice when disclosure is made to a third party that is acting as an agent to perform task(s) on behalf of and under the instructions of the organization. However, an organization shall always enter into a contract with the agent.
- c. For sensitive information (*i.e.*, personal information specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or information specifying the sex life of the individual), organizations must obtain affirmative express consent (*i.e.*, opt in) from individuals if such information is to be (i) disclosed to a third party or (ii) used for a purpose other than those for which it was originally collected or subsequently authorized by the individuals through the exercise of opt-in choice. In addition, an organization should treat as sensitive any personal information received from a third party where the third party identifies and treats it as sensitive.

3. ACCOUNTABILITY FOR ONWARD TRANSFER

- a. To transfer personal information to a third party acting as a controller, organizations must comply with the Notice and Choice Principles. Organizations must also enter into a contract with the third-party controller that provides that such data may only be processed for limited and specified purposes consistent with the consent provided by the individual and that the recipient will provide the same level of protection as the Principles and will notify the organization if it makes a determination that it can no longer meet this obligation. The contract shall provide that when such a determination is made the third party controller ceases processing or takes other reasonable and appropriate steps to remediate.
- b. To transfer personal data to a third party acting as an agent, organizations must: (i) transfer such data only for limited and specified purposes; (ii) ascertain that the agent is obligated to provide at least the same level of privacy protection as is required by the Principles; (iii) take reasonable and appropriate steps to ensure that the agent effectively processes the personal information transferred in a manner consistent with the organization's obligations under the Principles; (iv) require the agent to notify the organization if it makes a determination that it can no longer meet its obligation to provide the same level of protection as is required by the Principles; (v) upon notice, including under (iv), take reasonable and appropriate steps to stop and remediate unauthorized processing; and (vi) provide a summary or a representative copy of the relevant privacy provisions of its contract with that agent to the Department upon request.

4. SECURITY

- a. Organizations creating, maintaining, using or disseminating personal information must take reasonable and appropriate measures to protect it from loss, misuse and unauthorized access, disclosure, alteration and destruction, taking into due account the risks involved in the processing and the nature of the personal data.

5. DATA INTEGRITY AND PURPOSE LIMITATION

- a. Consistent with the Principles, personal information must be limited to the information that is relevant for the purposes of processing.⁶ An organization may not process personal information in a way that is incompatible with the purposes for which it has been collected or subsequently authorized by the individual. To the extent necessary for those purposes, an organization must take reasonable steps to ensure that personal data is reliable for its intended use, accurate, complete, and

⁶ Depending on the circumstances, examples of compatible processing purposes may include those that reasonably serve customer relations, compliance and legal considerations, auditing, security and fraud prevention, preserving or defending the organization's legal rights, or other purposes consistent with the expectations of a reasonable person given the context of the collection.

current. An organization must adhere to the Principles for as long as it retains such information.

- b. Information may be retained in a form identifying or making identifiable⁷ the individual only for as long as it serves a purpose of processing within the meaning of 5(a). This obligation does not prevent organizations from processing personal information for longer periods for the time and to the extent such processing reasonably serves the purposes of archiving in the public interest, journalism, literature and art, scientific or historical research, and statistical analysis. In these cases, such processing shall be subject to the other principles and provisions of the EU-U.S. DPF. Organizations should take reasonable and appropriate measures in complying with this provision.

6. ACCESS

- a. Individuals must have access to personal information about them that an organization holds and be able to correct, amend, or delete that information where it is inaccurate, or has been processed in violation of the Principles, except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question, or where the rights of persons other than the individual would be violated.

7. RECOURSE, ENFORCEMENT AND LIABILITY

- a. Effective privacy protection must include robust mechanisms for assuring compliance with the Principles, recourse for individuals who are affected by non-compliance with the Principles, and consequences for the organization when the Principles are not followed. At a minimum such mechanisms must include:
 - i. readily available independent recourse mechanisms by which each individual's complaints and disputes are investigated and expeditiously resolved at no cost to the individual and by reference to the Principles, and damages awarded where the applicable law or private-sector initiatives so provide;
 - ii. follow-up procedures for verifying that the attestations and assertions organizations make about their privacy practices are true and that privacy practices have been implemented as presented and, in particular, with regard to cases of non-compliance; and
 - iii. obligations to remedy problems arising out of failure to comply with the Principles by organizations announcing their adherence to them and consequences for such organizations. Sanctions

⁷ In this context, if, given the means of identification reasonably likely to be used (considering, among other things, the costs of and the amount of time required for identification and the available technology at the time of the processing) and the form in which the data is retained, an individual could reasonably be identified by the organization, or a third party if it would have access to the data, then the individual is "identifiable."

must be sufficiently rigorous to ensure compliance by organizations.

- b. Organizations and their selected independent recourse mechanisms will respond promptly to inquiries and requests by the Department for information relating to the EU-U.S. DPF. All organizations must respond expeditiously to complaints regarding compliance with the Principles referred by EU Member State authorities through the Department. Organizations that have chosen to cooperate with DPAs, including organizations that process human resources data, must respond directly to such authorities with regard to the investigation and resolution of complaints.
- c. Organizations are obligated to arbitrate claims and follow the terms as set forth in Annex I, provided that an individual has invoked binding arbitration by delivering notice to the organization at issue and following the procedures and subject to conditions set forth in Annex I.
- d. In the context of an onward transfer, a participating organization has responsibility for the processing of personal information it receives under the EU-U.S. DPF and subsequently transfers to a third party acting as an agent on its behalf. The participating organization shall remain liable under the Principles if its agent processes such personal information in a manner inconsistent with the Principles, unless the organization proves that it is not responsible for the event giving rise to the damage.
- e. When an organization becomes subject to a court order that is based on non-compliance or an order from a U.S. statutory body (*e.g.*, FTC or DOT) listed in the Principles or in a future annex to the Principles that is based on non-compliance, the organization shall make public any relevant EU-U.S. DPF-related sections of any compliance or assessment report submitted to the court or U.S. statutory body to the extent consistent with confidentiality requirements. The Department has established a dedicated point of contact for DPAs for any problems of compliance by participating organizations. The FTC and the DOT will give priority consideration to referrals of non-compliance with the Principles from the Department and EU Member State authorities, and will exchange information regarding referrals with the referring state authorities on a timely basis, subject to existing confidentiality restrictions.

III. SUPPLEMENTAL PRINCIPLES

1. Sensitive Data

- a. An organization is not required to obtain affirmative, express consent (*i.e.*, opt in) with respect to sensitive data where the processing is:
 - i. in the vital interests of the data subject or another person;
 - ii. necessary for the establishment of legal claims or defenses;
 - iii. required to provide medical care or diagnosis;
 - iv. carried out in the course of legitimate activities by a foundation, association or any other non-profit body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members of the body or to the persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects;
 - v. necessary to carry out the organization's obligations in the field of employment law; or
 - vi. related to data that are manifestly made public by the individual.

2. Journalistic Exceptions

- a. Given U.S. constitutional protections for freedom of the press, where the rights of a free press embodied in the First Amendment of the U.S. Constitution intersect with privacy protection interests, the First Amendment must govern the balancing of these interests with regard to the activities of U.S. persons or organizations.
- b. Personal information that is gathered for publication, broadcast, or other forms of public communication of journalistic material, whether used or not, as well as information found in previously published material disseminated from media archives, is not subject to the requirements of the Principles.

3. Secondary Liability

- a. Internet Service Providers ("ISPs"), telecommunications carriers, and other organizations are not liable under the Principles when on behalf of another organization they merely transmit, route, switch, or cache information. The EU-U.S. DPF does not create secondary liability. To the extent that an organization is acting as a mere conduit for data transmitted by third parties and does not determine the purposes and means of processing those personal data, it would not be liable.

4. Performing Due Diligence and Conducting Audits

- a. The activities of auditors and investment bankers may involve processing personal data without the consent or knowledge of the

individual. This is permitted by the Notice, Choice, and Access Principles under the circumstances described below.

- b. Public stock corporations and closely held companies, including participating organizations, are regularly subject to audits. Such audits, particularly those looking into potential wrongdoing, may be jeopardized if disclosed prematurely. Similarly, a participating organization involved in a potential merger or takeover will need to perform, or be the subject of, a “due diligence” review. This will often entail the collection and processing of personal data, such as information on senior executives and other key personnel. Premature disclosure could impede the transaction or even violate applicable securities regulation. Investment bankers and attorneys engaged in due diligence, or auditors conducting an audit, may process information without knowledge of the individual only to the extent and for the period necessary to meet statutory or public interest requirements and in other circumstances in which the application of these Principles would prejudice the legitimate interests of the organization. These legitimate interests include the monitoring of organizations’ compliance with their legal obligations and legitimate accounting activities, and the need for confidentiality connected with possible acquisitions, mergers, joint ventures, or other similar transactions carried out by investment bankers or auditors.

5. The Role of the Data Protection Authorities

- a. Organizations will implement their commitment to cooperate with DPAs as described below. Under the EU-U.S. DPF, U.S. organizations receiving personal data from the EU must commit to employ effective mechanisms for assuring compliance with the Principles. More specifically as set out in the Recourse, Enforcement and Liability Principle, participating organizations must provide: (a)(i) recourse for individuals to whom the data relate; (a)(ii) follow-up procedures for verifying that the attestations and assertions they have made about their privacy practices are true; and (a)(iii) obligations to remedy problems arising out of failure to comply with the Principles and consequences for such organizations. An organization may satisfy points (a)(i) and (a)(iii) of the Recourse, Enforcement and Liability Principle if it adheres to the requirements set forth here for cooperating with the DPAs.
- b. An organization commits to cooperate with the DPAs by declaring in its EU-U.S. DPF self-certification submission to the Department (*see* Supplemental Principle on Self-Certification) that the organization:
 - i. elects to satisfy the requirement in points (a)(i) and (a)(iii) of the Recourse, Enforcement and Liability Principle by committing to cooperate with the DPAs;
 - ii. will cooperate with the DPAs in the investigation and resolution of complaints brought under the Principles; and

iii. will comply with any advice given by the DPAs where the DPAs take the view that the organization needs to take specific action to comply with the Principles, including remedial or compensatory measures for the benefit of individuals affected by any non-compliance with the Principles, and will provide the DPAs with written confirmation that such action has been taken.

c. Operation of DPA Panels

i. The cooperation of the DPAs will be provided in the form of information and advice in the following way:

1. The advice of the DPAs will be delivered through an informal panel of DPAs established at the EU level, which will *inter alia* help ensure a harmonized and coherent approach.
2. The panel will provide advice to the U.S. organizations concerned on unresolved complaints from individuals about the handling of personal information that has been transferred from the EU under the EU-U.S. DPF. This advice will be designed to ensure that the Principles are being correctly applied and will include any remedies for the individual(s) concerned that the DPAs consider appropriate.
3. The panel will provide such advice in response to referrals from the organizations concerned and/or to complaints received directly from individuals against organizations which have committed to cooperate with DPAs for EU-U.S. DPF purposes, while encouraging and if necessary helping such individuals in the first instance to use the in-house complaint handling arrangements that the organization may offer.
4. Advice will be issued only after both sides in a dispute have had a reasonable opportunity to comment and to provide any evidence they wish. The panel will seek to deliver advice as quickly as this requirement for due process allows. As a general rule, the panel will aim to provide advice within 60 days after receiving a complaint or referral and more quickly where possible.
5. The panel will make public the results of its consideration of complaints submitted to it, if it sees fit.
6. The delivery of advice through the panel will not give rise to any liability for the panel or for individual DPAs.

ii. As noted above, organizations choosing this option for dispute resolution must undertake to comply with the advice of the DPAs. If an organization fails to comply within 25 days of the delivery of the advice and has offered no satisfactory explanation for the delay, the panel will give notice of its

intention either to refer the matter to the FTC, the DOT, or other U.S. federal or state body with statutory powers to take enforcement action in cases of deception or misrepresentation, or to conclude that the agreement to cooperate has been seriously breached and must therefore be considered null and void. In the latter case, the panel will inform the Department so that the Data Privacy Framework List can be duly amended. Any failure to fulfill the undertaking to cooperate with the DPAs, as well as failures to comply with the Principles, will be actionable as a deceptive practice under Section 5 of the FTC Act (15 U.S.C. § 45), 49 U.S.C. § 41712, or other similar statute.

- d. An organization that wishes its EU-U.S. DPF benefits to cover human resources data transferred from the EU in the context of the employment relationship must commit to cooperate with the DPAs with regard to such data (*see* Supplemental Principle on Human Resources Data).
- e. Organizations choosing this option will be required to pay an annual fee, which will be designed to cover the operating costs of the panel. They may additionally be asked to meet any necessary translation expenses arising out of the panel's consideration of referrals or complaints against them. The amount of the fee will be determined by the Department after consultation with the Commission. The collection of the fee may be conducted by a third party selected by the Department to serve as the custodian of the funds collected for this purpose. The Department will closely cooperate with the Commission and the DPAs on the establishment of appropriate procedures for the distribution of funds collected through the fee, as well as other procedural and administrative aspects of the panel. The Department and the Commission may agree to alter how often the fee is collected.

6. Self-Certification

- a. EU-U.S. DPF benefits are assured from the date on which the Department places the organization on the Data Privacy Framework List. The Department will only place an organization on the Data Privacy Framework List after having determined that the organization's initial self-certification submission is complete, and will remove the organization from that list if it voluntarily withdraws, fails to complete its annual re-certification, or if it persistently fails to comply with the Principles (*see* Supplemental Principle on Dispute Resolution and Enforcement).
- b. To initially self-certify or subsequently re-certify for the EU-U.S. DPF, an organization must on each occasion provide to the Department a submission by a corporate officer on behalf of the organization that is

self-certifying or re-certifying (as applicable) its adherence to the Principles⁸, that contains at least the following information:

- i. the name of the self-certifying or re-certifying U.S. organization, as well as the name(s) of any of its U.S. entities or U.S. subsidiaries also adhering to the Principles that the organization wishes to cover;
- ii. a description of the activities of the organization with respect to personal information that would be received from the EU under the EU-U.S. DPF;
- iii. a description of the organization’s relevant privacy policy/ies for such personal information, including:
 1. if the organization has a public website, the relevant web address where the privacy policy is available, or if the organization does not have a public website, where the privacy policy is available for viewing by the public; and
 2. its effective date of implementation;
- iv. a contact office within the organization for the handling of complaints, access requests, and any other issues arising under the Principles⁹, including:
 1. the name(s), job title(s) (as applicable), e-mail address(es), and telephone number(s) of the relevant individual(s) or relevant contact office(s) within the organization; and
 2. the relevant U.S. mailing address for the organization;
- v. the specific statutory body that has jurisdiction to hear any claims against the organization regarding possible unfair or deceptive practices and violations of laws or regulations governing privacy (and that is listed in the Principles or a future annex to the Principles);
- vi. the name of any privacy program in which the organization is a member;
- vii. the method of verification (*i.e.*, self-assessment; or outside compliance reviews, including the third party that completes such reviews);¹⁰ and
- viii. the relevant independent recourse mechanism(s) available to investigate unresolved Principles-related complaints.¹¹

⁸ The submission must be made via the Department’s Data Privacy Framework website by an individual within the organization who is authorized to make representations on behalf of the organization and any of its covered entities regarding its adherence to the Principles.

⁹ The primary “organization contact” or the “organization corporate officer” cannot be external to the organization (*e.g.*, outside counsel or an external consultant).

¹⁰ See Supplemental Principle on Verification.

¹¹ See Supplemental Principle on Dispute Resolution and Enforcement.

- c. Where the organization wishes its EU-U.S. DPF benefits to cover human resources information transferred from the EU for use in the context of the employment relationship, it may do so where a statutory body listed in the Principles or a future annex to the Principles has jurisdiction to hear claims against the organization arising out of the processing of human resources information. In addition, the organization must indicate this in its initial self-certification submission, as well as in any re-certification submissions, and declare its commitment to cooperate with the EU authority or authorities concerned in conformity with the Supplemental Principles on Human Resources Data and the Role of the Data Protection Authorities (as applicable) and that it will comply with the advice given by such authorities. The organization must also provide the Department with a copy of its human resources privacy policy and provide information where the privacy policy is available for viewing by its affected employees.
- d. The Department will maintain and make publicly available the Data Privacy Framework List of organizations that have filed completed, initial self-certification submissions and will update that list on the basis of completed, annual re-certification submissions, as well as notifications received pursuant to the Supplemental Principle on Dispute Resolution and Enforcement. Such re-certification submissions must be provided not less than annually; otherwise the organization will be removed from the Data Privacy Framework List and EU-U.S. DPF benefits will no longer be assured. All organizations that are placed on the Data Privacy Framework List by the Department must have relevant privacy policies that comply with the Notice Principle and state in those privacy policies that they adhere to the Principles.¹² If available online, an organization's privacy policy must include a hyperlink to the Department's Data Privacy Framework website and a hyperlink to the website or complaint submission form of the independent recourse mechanism that is available to investigate unresolved, Principles-related complaints free of charge to the individual.
- e. The Principles apply immediately upon self-certification. Participating organizations that previously self-certified to the EU-U.S. Privacy Shield Framework Principles will need to update their privacy policies to instead refer to the "EU-U.S. Data Privacy Framework Principles". Such organizations shall include this reference 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.

¹² An organization self-certifying for the first time may not claim EU-U.S. DPF participation in its final privacy policy until the Department notifies the organization that it may do so. The organization must provide the Department with a draft privacy policy, which is consistent with the Principles, when it submits its initial self-certification. Once the Department has determined that the organization's initial self-certification submission is otherwise complete, the Department will notify the organization that it should finalize (*e.g.*, publish where applicable) its EU-U.S. DPF-consistent privacy policy. The organization must promptly notify the Department as soon as the relevant privacy policy is finalized, at which time the Department will place the organization on the Data Privacy Framework List.

- f. An organization must subject to the Principles all personal data received from the EU in reliance on the EU-U.S. DPF. The undertaking to adhere to the Principles is not time-limited in respect of personal data received during the period in which the organization enjoys the benefits of the EU-U.S. DPF; its undertaking means that it will continue to apply the Principles to such data for as long as the organization stores, uses or discloses them, even if it subsequently leaves the EU-U.S. DPF for any reason. An organization that wishes to withdraw from the EU-U.S. DPF must notify the Department of this in advance. This notification must also indicate what the organization will do with the personal data that it received in reliance on the EU-U.S. DPF (*i.e.*, retain, return, or delete the data, and if it will retain the data, the authorized means by which it will provide protection to the data). An organization that withdraws from the EU-U.S. DPF, but wants to retain such data must either affirm to the Department on an annual basis its commitment to continue to apply the Principles to the data or provide “adequate” protection for the data by another authorized means (for example, using a contract that fully reflects the requirements of the relevant standard contractual clauses adopted by the Commission); otherwise, the organization must return or delete the information.¹³ An organization that withdraws from the EU-U.S. DPF must remove from any relevant privacy policy any references to the EU-U.S. DPF that imply that the organization continues to participate in the EU-U.S. DPF and is entitled to its benefits.
- g. An organization that will cease to exist as a separate legal entity due to a change in corporate status, such as a result of a merger, takeover, bankruptcy, or dissolution must notify the Department of this in advance. The notification should also indicate whether the entity resulting from the change in corporate status will (i) continue to participate in the EU-U.S. DPF through an existing self-certification; (ii) self-certify as a new participant in the EU-U.S. DPF (*e.g.*, where the new entity or surviving entity does not already have an existing self-certification through which it could participate in the EU-U.S. DPF); or (iii) put in place other safeguards, such as a written agreement that will ensure continued application of the Principles to any personal data that the organization received under the EU-U.S. DPF and will be retained. Where neither (i), (ii), nor (iii) applies, any personal data that has been received under the EU-U.S. DPF must be promptly returned or deleted.
- h. When an organization leaves the EU-U.S. DPF for any reason, it must remove all statements implying that the organization continues to participate in the EU-U.S. DPF or is entitled to the benefits of the EU-U.S. DPF. The EU-U.S. DPF certification mark, if used, must also be

¹³ If an organization elects at the time of its withdrawal to retain the personal data that it received in reliance on the EU-U.S. DPF and affirm to the Department on an annual basis that it continues to apply the Principles to such data, the organization must verify to the Department once a year following its withdrawal (*i.e.*, unless and until the organization provides “adequate” protection for such data by another authorized means, or returns or deletes all such data and notifies the Department of this action) 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 will serve as an ongoing point of contact for Principles-related questions.

removed. Any misrepresentation to the general public concerning an organization's adherence to the Principles may be actionable by the FTC, DOT, or other relevant government body. Misrepresentations to the Department may be actionable under the False Statements Act (18 U.S.C. § 1001).

7. Verification

- a. Organizations must provide follow-up procedures for verifying that the attestations and assertions they make about their EU-U.S. DPF privacy practices are true and those privacy practices have been implemented as represented and in accordance with the Principles.
- b. To meet the verification requirements of the Recourse, Enforcement and Liability Principle, an organization must verify such attestations and assertions either through self-assessment or outside compliance reviews.
- c. Where the organization has chosen self-assessment, such verification must demonstrate that its privacy policy regarding personal information received from the EU is accurate, comprehensive, readily available, conforms to the Principles, and is completely implemented (*i.e.*, is being complied with). It must also indicate that individuals are informed of any in-house arrangements for handling complaints and of the independent recourse mechanism(s) through which they may pursue complaints; that it has in place procedures for training employees in its implementation, and disciplining them for failure to follow it; and that it has in place internal procedures for periodically conducting objective reviews of compliance with the above. A statement verifying that the self-assessment has been completed must be signed by a corporate officer or other authorized representative of the organization at least once a year and made available upon request by individuals or in the context of an investigation or a complaint about non-compliance.
- d. Where the organization has chosen outside compliance review, such verification must demonstrate that its privacy policy regarding personal information received from the EU is accurate, comprehensive, readily available, conforms to the Principles, and is completely implemented (*i.e.*, is being complied with). It must also indicate that individuals are informed of mechanism(s) through which they may pursue complaints. The methods of review may include, without limitation, auditing, random reviews, use of "decoys", or use of technology tools as appropriate. A statement verifying that an outside compliance review has been successfully completed must be signed either by the reviewer or by the corporate officer or other authorized representative of the organization at least once a year and made available upon request by individuals or in the context of an investigation or a complaint about compliance.
- e. Organizations must retain their records on the implementation of their EU-U.S. DPF privacy practices and make them available upon request in the context of an investigation or a complaint about non-compliance

to the independent dispute resolution body responsible for investigating complaints or to the agency with unfair and deceptive practices jurisdiction. Organizations must also respond promptly to inquiries and other requests for information from the Department relating to the organization's adherence to the Principles.

8. Access

a. The Access Principle in Practice

- i. Under the Principles, the right of access is fundamental to privacy protection. In particular, it allows individuals to verify the accuracy of information held about them. The Access Principle means that individuals have the right to:
 1. obtain from an organization confirmation of whether or not the organization is processing personal data relating to them;¹⁴
 2. have communicated to them such data so that they could verify its accuracy and the lawfulness of the processing; and
 3. have the data corrected, amended or deleted where it is inaccurate or processed in violation of the Principles.
- ii. Individuals do not have to justify requests for access to their personal data. In responding to individuals' access requests, organizations should first be guided by the concern(s) that led to the requests in the first place. For example, if an access request is vague or broad in scope, an organization may engage the individual in a dialogue so as to better understand the motivation for the request and to locate responsive information. The organization might inquire about which part(s) of the organization the individual interacted with or about the nature of the information or its use that is the subject of the access request.
- iii. Consistent with the fundamental nature of access, organizations should always make good faith efforts to provide access. For example, where certain information needs to be protected and can be readily separated from other personal information subject to an access request, the organization should redact the protected information and make available the other information. If an organization determines that access should be restricted in any particular instance, it should provide the individual requesting access with an explanation of why it has made that determination and a contact point for any further inquiries.

¹⁴ The organization should answer requests from an individual concerning the purposes of the processing, the categories of personal data concerned, and the recipients or categories of recipients to whom the personal data is disclosed.

b. Burden or Expense of Providing Access

- i. The right of access to personal data may be restricted in exceptional circumstances where the legitimate rights of persons other than the individual would be violated or where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question. Expense and burden are important factors and should be taken into account but they are not controlling factors in determining whether providing access is reasonable.
- ii. For example, if the personal information is used for decisions that will significantly affect the individual (*e.g.*, the denial or grant of important benefits, such as insurance, a mortgage, or a job), then consistent with the other provisions of these Supplemental Principles, the organization would have to disclose that information even if it is relatively difficult or expensive to provide. If the personal information requested is not sensitive or not used for decisions that will significantly affect the individual, but is readily available and inexpensive to provide, an organization would have to provide access to such information.

c. Confidential Commercial Information

- i. Confidential commercial information is information that an organization has taken steps to protect from disclosure, where disclosure would help a competitor in the market. Organizations may deny or limit access to the extent that granting full access would reveal its own confidential commercial information, such as marketing inferences or classifications generated by the organization, or the confidential commercial information of another that is subject to a contractual obligation of confidentiality.
- ii. Where confidential commercial information can be readily separated from other personal information subject to an access request, the organization should redact the confidential commercial information and make available the non-confidential information.

d. Organization of Data Bases

- i. Access can be provided in the form of disclosure of the relevant personal information by an organization to the individual and does not require access by the individual to an organization's data base.
- ii. Access needs to be provided only to the extent that an organization stores the personal information. The Access Principle does not itself create any obligation to retain, maintain, reorganize, or restructure personal information files.

e. When Access May be Restricted

- i. As organizations must always make good faith efforts to provide individuals with access to their personal data, the circumstances in which organizations may restrict such access are limited, and any reasons for restricting access must be specific. As under the GDPR, an organization can restrict access to information to the extent that disclosure is likely to interfere with the safeguarding of important countervailing public interests, such as national security; defense; or public security. In addition, where personal information is processed solely for research or statistical purposes, access may be denied. Other reasons for denying or limiting access are:
 1. interference with the execution or enforcement of the law or with private causes of action, including the prevention, investigation or detection of offenses or the right to a fair trial;
 2. disclosure where the legitimate rights or important interests of others would be violated;
 3. breaching a legal or other professional privilege or obligation;
 4. prejudicing employee security investigations or grievance proceedings or in connection with employee succession planning and corporate re-organizations; or
 5. prejudicing the confidentiality necessary in monitoring, inspection or regulatory functions connected with sound management, or in future or ongoing negotiations involving the organization.
- ii. An organization which claims an exception has the burden of demonstrating its necessity, and the reasons for restricting access and a contact point for further inquiries should be given to individuals.

f. Right to Obtain Confirmation and Charging a Fee to Cover the Costs for Providing Access

- i. An individual has the right to obtain confirmation of whether or not this organization has personal data relating to him or her. An individual also has the right to have communicated to him or her personal data relating to him or her. An organization may charge a fee that is not excessive.
- ii. Charging a fee may be justified, for example, where requests for access are manifestly excessive, in particular because of their repetitive character.
- iii. Access may not be refused on cost grounds if the individual offers to pay the costs.

- g. Repetitious or Vexatious Requests for Access
 - i. An organization may set reasonable limits on the number of times within a given period that access requests from a particular individual will be met. In setting such limitations, an organization should consider such factors as the frequency with which information is updated, the purpose for which the data are used, and the nature of the information.
- h. Fraudulent Requests for Access
 - i. An organization is not required to provide access unless it is supplied with sufficient information to allow it to confirm the identity of the person making the request.
- i. Timeframe for Responses
 - i. Organizations should respond to access requests within a reasonable time period, in a reasonable manner, and in a form that is readily intelligible to the individual. An organization that provides information to data subjects at regular intervals may satisfy an individual access request with its regular disclosure if it would not constitute an excessive delay.

9. Human Resources Data

- a. Coverage by the EU-U.S. DPF
 - i. Where an organization in the EU transfers personal information about its employees (past or present) collected in the context of the employment relationship, to a parent, affiliate, or unaffiliated service provider in the United States participating in the EU-U.S. DPF, the transfer enjoys the benefits of the EU-U.S. DPF. In such cases, the collection of the information and its processing prior to transfer will have been subject to the national laws of the EU Member State where it was collected, and any conditions for or restrictions on its transfer according to those laws will have to be respected.
 - ii. The Principles are relevant only when individually identified or identifiable records are transferred or accessed. Statistical reporting relying on aggregate employment data and containing no personal data or the use of anonymized data does not raise privacy concerns.
- b. Application of the Notice and Choice Principles
 - i. A U.S. organization that has received employee information from the EU under the EU-U.S. DPF may disclose it to third parties or use it for different purposes only in accordance with the Notice and Choice Principles. For example, where an organization intends to use personal information collected through the employment relationship for non-employment-related purposes, such as marketing communications, the U.S.

organization must provide the affected individuals with the requisite choice before doing so, unless they have already authorized the use of the information for such purposes. Such use must not be incompatible with the purposes for which the personal information has been collected or subsequently authorized by the individual. Moreover, such choices must not be used to restrict employment opportunities or take any punitive action against such employees.

- ii. It should be noted that certain generally applicable conditions for transfer from some EU Member States may preclude other uses of such information even after transfer outside the EU and such conditions will have to be respected.
- iii. In addition, employers should make reasonable efforts to accommodate employee privacy preferences. This could include, for example, restricting access to the personal data, anonymizing certain data, or assigning codes or pseudonyms when the actual names are not required for the management purpose at hand.
- iv. To the extent and for the period necessary to avoid prejudicing the ability of the organization in making promotions, appointments, or other similar employment decisions, an organization does not need to offer notice and choice.

c. Application of the Access Principle

- i. The Supplemental Principle on Access provides guidance on reasons which may justify denying or limiting access on request in the human resources context. Of course, employers in the EU must comply with local regulations and ensure that EU employees have access to such information as is required by law in their home countries, regardless of the location of data processing and storage. The EU-U.S. DPF requires that an organization processing such data in the United States will cooperate in providing such access either directly or through the EU employer.

d. Enforcement

- i. In so far as personal information is used only in the context of the employment relationship, primary responsibility for the data vis-à-vis the employee remains with the organization in the EU. It follows that, where European employees make complaints about violations of their data protection rights and are not satisfied with the results of internal review, complaint, and appeal procedures (or any applicable grievance procedures under a contract with a trade union), they should be directed to the state or national data protection or labor authority in the jurisdiction where the employees work. This includes cases where the alleged mishandling of their personal information is the responsibility of the U.S. organization that has received the

information from the employer and thus involves an alleged breach of the Principles. This will be the most efficient way to address the often overlapping rights and obligations imposed by local labor law and labor agreements as well as data protection law.

- ii. A U.S. organization participating in the EU-U.S. DPF that uses EU human resources data transferred from the EU in the context of the employment relationship and that wishes such transfers to be covered by the EU-U.S. DPF must therefore commit to cooperate in investigations by and to comply with the advice of competent EU authorities in such cases.
- e. Application of the Accountability for Onward Transfer Principle
 - i. For occasional employment-related operational needs of the participating organization with respect to personal data transferred under the EU-U.S. DPF, such as the booking of a flight, hotel room, or insurance coverage, transfers of personal data of a small number of employees can take place to controllers without application of the Access Principle or entering into a contract with the third-party controller, as otherwise required under the Accountability for Onward Transfer Principle, provided that the participating organization has complied with the Notice and Choice Principles.

10. Obligatory Contracts for Onward Transfers

- a. Data Processing Contracts
 - i. When personal data is transferred from the EU to the United States only for processing purposes, a contract will be required, regardless of participation by the processor in the EU-U.S. DPF.
 - ii. Data controllers in the EU are always required to enter into a contract when a transfer for mere processing is made, whether the processing operation is carried out inside or outside the EU, and whether or not the processor participates in the EU-U.S. DPF. The purpose of the contract is to make sure that the processor:
 - 1. acts only on instructions from the controller;
 - 2. provides appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, and understands whether onward transfer is allowed; and
 - 3. taking into account the nature of the processing, assists the controller in responding to individuals exercising their rights under the Principles.

- iii. Because adequate protection is provided by participating organizations, contracts with such organizations for mere processing do not require prior authorization.
- b. Transfers within a Controlled Group of Corporations or Entities
 - i. When personal information is transferred between two controllers within a controlled group of corporations or entities, a contract is not always required under the Accountability for Onward Transfer Principle. Data controllers within a controlled group of corporations or entities may base such transfers on other instruments, such as EU Binding Corporate Rules or other intra-group instruments (*e.g.*, compliance and control programs), ensuring the continuity of protection of personal information under the Principles. In case of such transfers, the participating organization remains responsible for compliance with the Principles.
- c. Transfers between Controllers
 - i. For transfers between controllers, the recipient controller need not be a participating organization or have an independent recourse mechanism. The participating organization must enter into a contract with the recipient third-party controller that provides for the same level of protection as is available under the EU-U.S. DPF, not including the requirement that the third party controller be a participating organization or have an independent recourse mechanism, provided it makes available an equivalent mechanism.

11. Dispute Resolution and Enforcement

- a. The Recourse, Enforcement and Liability Principle sets out the requirements for EU-U.S. DPF enforcement. How to meet the requirements of point (a)(ii) of the Principle is set out in the Supplemental Principle on Verification. This Supplemental Principle addresses points (a)(i) and (a)(iii), both of which require independent recourse mechanisms. These mechanisms may take different forms, but they must meet the Recourse, Enforcement and Liability Principle's requirements. Organizations satisfy the requirements through the following: (i) compliance with private sector developed privacy programs that incorporate the Principles into their rules and that include effective enforcement mechanisms of the type described in the Recourse, Enforcement and Liability Principle; (ii) compliance with legal or regulatory supervisory authorities that provide for handling of individual complaints and dispute resolution; or (iii) commitment to cooperate with DPAs located in the EU or their authorized representatives.
- b. This list is intended to be illustrative and not limiting. The private sector may design additional mechanisms to provide enforcement, so long as they meet the requirements of the Recourse, Enforcement and Liability

Principle and the Supplemental Principles. Please note that the Recourse, Enforcement and Liability Principle's requirements are additional to the requirement that self-regulatory efforts must be enforceable under Section 5 of the FTC Act (15 U.S.C. § 45) prohibiting unfair or deceptive acts, 49 U.S.C. § 41712 prohibiting a carrier or ticket agent from engaging in an unfair or deceptive practice in air transportation or the sale of air transportation, or another law or regulation prohibiting such acts.

- c. In order to help ensure compliance with their EU-U.S. DPF commitments and to support the administration of the program, organizations, as well as their independent recourse mechanisms, must provide information relating to the EU-U.S. DPF when requested by the Department. In addition, organizations must respond expeditiously to complaints regarding their compliance with the Principles referred through the Department by DPAs. The response should address whether the complaint has merit and, if so, how the organization will rectify the problem. The Department will protect the confidentiality of information it receives in accordance with U.S. law.
- d. Recourse Mechanisms
 - i. Individuals should be encouraged to raise any complaints they may have with the relevant organization before proceeding to independent recourse mechanisms. Organizations must respond to an individual within 45 days of receiving a complaint. Whether a recourse mechanism is independent is a factual question that can be demonstrated notably by impartiality, transparent composition and financing, and a proven track record. As required by the Recourse, Enforcement and Liability Principle, the recourse available to individuals must be readily available and free of charge to individuals. Independent dispute resolution bodies should look into each complaint received from individuals unless they are obviously unfounded or frivolous. This does not preclude the establishment of eligibility requirements by the independent dispute resolution body operating the recourse mechanism, but such requirements should be transparent and justified (for example, to exclude complaints that fall outside the scope of the program or are for consideration in another forum), and should not have the effect of undermining the commitment to look into legitimate complaints. In addition, recourse mechanisms should provide individuals with full and readily available information about how the dispute resolution procedure works when they file a complaint. Such information should include notice about the mechanism's privacy practices, in conformity with the Principles. They should also cooperate in the development of tools, such as standard complaint forms to facilitate the complaint resolution process.
 - ii. Independent recourse mechanisms must include on their public websites information regarding the Principles and the services that they provide under the EU-U.S. DPF. This information

must include: (1) information on or a link to the Principles' requirements for independent recourse mechanisms; (2) a link to the Department's Data Privacy Framework website; (3) an explanation that their dispute resolution services under the EU-U.S. DPF 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.

iii. Independent recourse mechanisms must publish an annual report providing aggregate statistics regarding their dispute resolution services. The annual report 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.

iv. As set forth in Annex I, an arbitration option is available to an individual to determine, for residual claims, whether a participating organization has violated its obligations under the Principles as to that individual, and whether any such violation remains fully or partially unremedied. This option is available only for these purposes. This option is not available, for example, with respect to the exceptions to the Principles¹⁵ or with respect to an allegation about the adequacy of the EU-U.S. DPF. Under this arbitration option, the "EU-U.S. Data Privacy Framework Panel" (consisting of one or three arbitrators, as agreed by the parties) has the authority to impose individual-specific, non-monetary equitable relief (such as access, correction, deletion, or return of the individual's data in question) necessary to remedy the violation of the Principles only with respect to the individual. Individuals and participating organizations will be able to seek judicial review and enforcement of the arbitral decisions pursuant to U.S. law under the Federal Arbitration Act.

e. Remedies and Sanctions

i. The result of any remedies provided by the independent dispute resolution body should be that the effects of non-compliance are reversed or corrected by the organization, insofar as feasible, and that future processing by the organization will be in conformity with the Principles and, where appropriate, that processing of the personal data of the individual who brought the complaint will cease. Sanctions need to be rigorous enough to ensure compliance by the organization with the Principles. A range of sanctions of varying degrees of severity will allow dispute resolution bodies to respond appropriately to varying degrees of non-compliance. Sanctions should include both

¹⁵ The Principles, Overview, para. 5.

publicity for findings of non-compliance and the requirement to delete data in certain circumstances.¹⁶ Other sanctions could include suspension and removal of a seal, compensation for individuals for losses incurred as a result of non-compliance and injunctive awards. Private-sector independent dispute resolution bodies and self-regulatory bodies must notify failures of participating organizations to comply with their rulings to the governmental body with applicable jurisdiction or the courts, as appropriate, and the Department.

f. FTC Action

- i. The FTC has committed to reviewing on a priority basis referrals alleging non-compliance with the Principles received from: (i) privacy self-regulatory bodies and other independent dispute resolution bodies; (ii) EU Member States; and (iii) the Department, to determine whether Section 5 of the FTC Act prohibiting unfair or deceptive acts or practices in commerce has been violated. If the FTC concludes that it has reason to believe Section 5 has been violated, it may resolve the matter by seeking an administrative cease and desist order prohibiting the challenged practices or by filing a complaint in a federal district court, which if successful could result in a federal court order to same effect. This includes false claims of adherence to the Principles or participation in the EU-U.S. DPF by organizations, which either are no longer on the Data Privacy Framework List or have never self-certified to the Department. The FTC may obtain civil penalties for violations of an administrative cease and desist order and may pursue civil or criminal contempt for violation of a federal court order. The FTC will notify the Department of any such actions it takes. The Department encourages other government bodies to notify it of the final disposition of any such referrals or other rulings determining adherence to the Principles.

g. Persistent Failure to Comply

- i. If an organization persistently fails to comply with the Principles, it is no longer entitled to benefit from the EU-U.S. DPF. Organizations that have persistently failed to comply with the Principles will be removed from the Data Privacy Framework List by the Department and must return or delete the personal information they received under the EU-U.S. DPF.
- ii. Persistent failure to comply arises where an organization that has self-certified to the Department refuses to comply with a final determination by any privacy self-regulatory, independent dispute resolution, or government body, or where such a body,

¹⁶ Independent dispute resolution bodies have discretion about the circumstances in which they use these sanctions. The sensitivity of the data concerned is one factor to be taken into consideration in deciding whether deletion of data should be required, as is whether an organization has collected, used, or disclosed information in blatant contravention of the Principles.

including the Department, determines that an organization frequently fails to comply with the Principles to the point where its claim to comply is no longer credible. In cases where such a determination is made by a body other than the Department the organization must promptly notify the Department of such facts. Failure to do so may be actionable under the False Statements Act (18 U.S.C. § 1001). An organization's withdrawal from a private-sector privacy self-regulatory program or independent dispute resolution mechanism does not relieve it of its obligation to comply with the Principles and would constitute a persistent failure to comply.

- iii. The Department will remove an organization from the Data Privacy Framework List for persistent failure to comply, including in response to any notification it receives of such non-compliance from the organization itself, a privacy self-regulatory body or another independent dispute resolution body, or a government body, but only after first providing the organization with 30 days' notice and an opportunity to respond¹⁷. Accordingly, the Data Privacy Framework List maintained by the Department will make clear which organizations are assured and which organizations are no longer assured of EU-U.S. DPF benefits.
- iv. An organization applying to participate in a self-regulatory body for the purposes of requalifying for the EU-U.S. DPF must provide that body with full information about its prior participation in the EU-U.S. DPF.

12. Choice – Timing of Opt Out

- a. Generally, the purpose of the Choice Principle is to ensure that personal information is used and disclosed in ways that are consistent with the individual's expectations and choices. Accordingly, an individual should be able to exercise "opt out" choice of having personal information used for direct marketing at any time subject to reasonable limits established by the organization, such as giving the organization time to make the opt out effective. An organization may also require sufficient information to confirm the identity of the individual requesting the "opt out." In the United States, individuals may be able to exercise this option through the use of a central "opt out" program. In any event, an individual should be given a readily available and affordable mechanism to exercise this option.
- b. Similarly, an organization may use information for certain direct marketing purposes when it is impracticable to provide the individual with an opportunity to opt out before using the information, if the organization promptly gives the individual such opportunity at the same time (and upon request at any time) to decline (at no cost to the

¹⁷ The Department will indicate within the notice the amount of time, which will necessarily be less than 30 days, the organization has to respond to the notice.

individual) to receive any further direct marketing communications and the organization complies with the individual's wishes.

13. Travel Information

- a. Airline passenger reservation and other travel information, such as frequent flyer or hotel reservation information and special handling needs, such as meals to meet religious requirements or physical assistance, may be transferred to organizations located outside the EU in several different circumstances. Under the GDPR, personal data may, in the absence of an adequacy decision, be transferred to a third country if appropriate data protection safeguards are provided pursuant to Article 46 GDPR or, in specific situations, if one of the conditions of Article 49 GDPR is fulfilled (*e.g.*, where the data subject has explicitly consented to the transfer). U.S. organizations subscribing to the EU-U.S. DPF provide adequate protection for personal data and may therefore receive data transfers from the EU on the basis of Article 45 GDPR, without having to put in place a transfer instrument pursuant to Article 46 GDPR or meet the conditions of Article 49 GDPR. Since the EU-U.S. DPF includes specific rules for sensitive information, such information (which may need to be collected, for example, in connection with customers' needs for physical assistance) may be included in transfers to participating organizations. In all cases, however, the organization transferring the information has to respect the law in the EU Member State in which it is operating, which may *inter alia* impose special conditions for the handling of sensitive data.

14. Pharmaceutical and Medical Products

- a. Application of EU/Member State Laws or the Principles
 - i. EU/Member State law applies to the collection of the personal data and to any processing that takes place prior to the transfer to the United States. The Principles apply to the data once they have been transferred to the United States. Data used for pharmaceutical research and other purposes should be anonymized when appropriate.
- b. Future Scientific Research
 - i. Personal data developed in specific medical or pharmaceutical research studies often play a valuable role in future scientific research. Where personal data collected for one research study are transferred to a U.S. organization in the EU-U.S. DPF, the organization may use the data for a new scientific research activity if appropriate notice and choice have been provided in the first instance. Such notice should provide information about any future specific uses of the data, such as periodic follow up, related studies, or marketing.
 - ii. It is understood that not all future uses of the data can be specified, since a new research use could arise from new insights

on the original data, new medical discoveries and advances, and public health and regulatory developments. Where appropriate, the notice should therefore include an explanation that personal data may be used in future medical and pharmaceutical research activities that are unanticipated. If the use is not consistent with the general research purpose(s) for which the personal data were originally collected, or to which the individual has consented subsequently, new consent must be obtained.

c. Withdrawal from a Clinical Trial

- i. Participants may decide or be asked to withdraw from a clinical trial at any time. Any personal data collected previous to withdrawal may still be processed along with other data collected as part of the clinical trial, however, if this was made clear to the participant in the notice at the time he or she agreed to participate.

d. Transfers for Regulatory and Supervision Purposes

- i. Pharmaceutical and medical device companies are allowed to provide personal data from clinical trials conducted in the EU to regulators in the United States for regulatory and supervision purposes. Similar transfers are allowed to parties other than regulators, such as company locations and other researchers, consistent with the Principles of Notice and Choice.

e. “Blinded” Studies

- i. To ensure objectivity in many clinical trials, participants, and often investigators as well, cannot be given access to information about which treatment each participant may be receiving. Doing so would jeopardize the validity of the research study and results. Participants in such clinical trials (referred to as “blinded” studies) do not have to be provided access to the data on their treatment during the trial if this restriction has been explained when the participant entered the trial and the disclosure of such information would jeopardize the integrity of the research effort.
- ii. Agreement to participate in the trial under these conditions is a reasonable forgoing of the right of access. Following the conclusion of the trial and analysis of the results, participants should have access to their data if they request it. They should seek it primarily from the physician or other health care provider from whom they received treatment within the clinical trial, or secondarily from the sponsoring organization.

f. Product Safety and Efficacy Monitoring

- i. A pharmaceutical or medical device company does not have to apply the Principles with respect to the Notice, Choice, Accountability for Onward Transfer, and Access Principles in its product safety and efficacy monitoring activities, including

the reporting of adverse events and the tracking of patients/subjects using certain medicines or medical devices, to the extent that adherence to the Principles interferes with compliance with regulatory requirements. This is true both with respect to reports by, for example, health care providers to pharmaceutical and medical device companies, and with respect to reports by pharmaceutical and medical device companies to government agencies like the Food and Drug Administration.

g. Key-coded Data

- i. Invariably, research data are uniquely key-coded at their origin by the principal investigator so as not to reveal the identity of individual data subjects. Pharmaceutical companies sponsoring such research do not receive the key. The unique key code is held only by the researcher, so that he or she can identify the research subject under special circumstances (*e.g.*, if follow-up medical attention is required). A transfer from the EU to the United States of data coded in this way that is EU personal data under EU law would be covered by the Principles.

15. Public Record and Publicly Available Information

- a. An organization must apply the Principles of Security, Data Integrity and Purpose Limitation, and Recourse, Enforcement and Liability to personal data from publicly available sources. These Principles shall apply also to personal data collected from public records (*i.e.*, those records kept by government agencies or entities at any level that are open to consultation by the public in general).
- b. It is not necessary to apply the Notice, Choice, or Accountability for Onward Transfer Principles to public record information, as long as it is not combined with non-public record information, and any conditions for consultation established by the relevant jurisdiction are respected. Also, it is generally not necessary to apply the Notice, Choice, or Accountability for Onward Transfer Principles to publicly available information unless the European transferor indicates that such information is subject to restrictions that require application of those Principles by the organization for the uses it intends. Organizations will have no liability for how such information is used by those obtaining such information from published materials.
- c. Where an organization is found to have intentionally made personal information public in contravention of the Principles so that it or others may benefit from these exceptions, it will cease to qualify for the benefits of the EU-U.S. DPF.
- d. It is not necessary to apply the Access Principle to public record information as long as it is not combined with other personal information (apart from small amounts used to index or organize the public record information); however, any conditions for consultation established by the relevant jurisdiction are to be respected. In contrast,

where public record information is combined with other non-public record information (other than as specifically noted above), an organization must provide access to all such information, assuming it is not subject to other permitted exceptions.

- e. As with public record information, it is not necessary to provide access to information that is already publicly available to the public at large, as long as it is not combined with non-publicly available information. Organizations that are in the business of selling publicly available information may charge the organization's customary fee in responding to requests for access. Alternatively, individuals may seek access to their information from the organization that originally compiled the data.

16. Access Requests by Public Authorities

- a. In order to provide transparency in respect of lawful requests by public authorities to access personal information, participating organizations may voluntarily issue periodic transparency reports on the number of requests for personal information they receive by public authorities for law enforcement or national security reasons, to the extent such disclosures are permissible under applicable law.
- b. The information provided by the participating organizations in these reports together with information that has been released by the intelligence community, along with other information, can be used to inform the periodic joint review of the functioning of the EU-U.S. DPF in accordance with the Principles.
- c. Absence of notice in accordance with point (a)(xii) of the Notice Principle shall not prevent or impair an organization's ability to respond to any lawful request.

ANNEX I: ARBITRAL MODEL

This Annex I provides the terms under which organizations participating in the EU-U.S. DPF are obligated to arbitrate claims, pursuant to the Recourse, Enforcement and Liability Principle. The binding arbitration option described below applies to certain “residual” claims as to data covered by the EU-U.S. DPF. The purpose of this option is to provide a prompt, independent, and fair mechanism, at the option of individuals, for resolution of any claimed violations of the Principles not resolved by any of the other EU-U.S. DPF mechanisms.

A. Scope

This arbitration option is available to an individual to determine, for residual claims, whether a participating organization has violated its obligations under the Principles as to that individual, and whether any such violation remains fully or partially unremedied. This option is available only for these purposes. This option is not available, for example, with respect to the exceptions to the Principles¹⁸ or with respect to an allegation about the adequacy of the EU-U.S. DPF.

B. Available Remedies

Under this arbitration option, the “EU-U.S. Data Privacy Framework Panel” (the arbitration panel consisting of one or three arbitrators, as agreed by the parties) has the authority to impose individual-specific, non-monetary equitable relief (such as access, correction, deletion, or return of the individual’s data in question) necessary to remedy the violation of the Principles only with respect to the individual. These are the only powers of the EU-U.S. Data Privacy Framework Panel with respect to remedies. In considering remedies, the EU-U.S. Data Privacy Framework Panel is required to consider other remedies that already have been imposed by other mechanisms under the EU-U.S. DPF. No damages, costs, fees, or other remedies are available. Each party bears its own attorney’s fees.

C. Pre-Arbitration Requirements

An individual who decides to invoke this arbitration option must take the following steps prior to initiating an arbitration claim: (1) raise the claimed violation directly with the organization and afford the organization an opportunity to resolve the issue within the timeframe set forth in section (d)(i) of the Supplemental Principle on Dispute Resolution and Enforcement; (2) make use of the independent recourse mechanism under the Principles, at no cost to the individual; and (3) raise the issue through the individual’s DPA to the Department and afford the Department an opportunity to use best efforts to resolve the issue within the timeframes set forth in the Letter from the Department’s International Trade Administration, at no cost to the individual.

This arbitration option may not be invoked if the individual’s same claimed violation of the Principles (1) has previously been subject to binding arbitration; (2) was the subject of a final judgment entered in a court action to which the individual was a party; or (3) was previously settled by the parties. In addition, this option may not be invoked if a DPA (1) has authority under the Supplemental Principle on the Role of the Data Protection Authorities or the Supplemental Principle on Human Resources Data; or (2) has the authority to resolve the claimed violation directly with the organization. A DPA’s authority to resolve the same

¹⁸ The Principles, Overview, para. 5.

claim against an EU data controller does not alone preclude invocation of this arbitration option against a different legal entity not bound by the DPA authority.

D. Binding Nature of Decisions

An individual's decision to invoke this binding arbitration option is entirely voluntary. Arbitral decisions will be binding on all parties to the arbitration. Once invoked, the individual forgoes the option to seek relief for the same claimed violation in another forum, except that if non-monetary equitable relief does not fully remedy the claimed violation, the individual's invocation of arbitration will not preclude a claim for damages that is otherwise available in the courts.

E. Review and Enforcement

Individuals and participating organizations will be able to seek judicial review and enforcement of the arbitral decisions pursuant to U.S. law under the Federal Arbitration Act.¹⁹ Any such cases must be brought in the federal district court whose territorial coverage includes the primary place of business of the participating organization.

This arbitration option is intended to resolve individual disputes, and arbitral decisions are not intended to function as persuasive or binding precedent in matters involving other parties, including in future arbitrations or in EU or U.S. courts, or FTC proceedings.

F. The Arbitration Panel

The parties will select arbitrators for the EU-U.S. Data Privacy Framework Panel from the list of arbitrators discussed below.

¹⁹ Chapter 2 of the Federal Arbitration Act ("FAA") provides that "[a]n arbitration agreement or arbitral award arising out of a legal relationship, whether contractual or not, which is considered as commercial, including a transaction, contract, or agreement described in [section 2 of the FAA], falls under the Convention [on the Recognition and Enforcement of Foreign Arbitral Awards of June 10, 1958, 21 U.S.T. 2519, T.I.A.S. No. 6997 ("New York Convention").]" 9 U.S.C. § 202. The FAA further provides that "[a]n agreement or award arising out of such a relationship which is entirely between citizens of the United States shall be deemed not to fall under the [New York] Convention unless that relationship involves property located abroad, envisages performance or enforcement abroad, or has some other reasonable relation with one or more foreign states." *Id.* Under Chapter 2, "any party to the arbitration may apply to any court having jurisdiction under this chapter for an order confirming the award as against any other party to the arbitration. The court shall confirm the award unless it finds one of the grounds for refusal or deferral of recognition or enforcement of the award specified in the said [New York] Convention." *Id.* § 207. Chapter 2 further provides that "[t]he district courts of the United States . . . shall have original jurisdiction over . . . an action or proceeding [under the New York Convention], regardless of the amount in controversy." *Id.* § 203.

Chapter 2 also provides that "Chapter 1 applies to actions and proceedings brought under this chapter to the extent that chapter is not in conflict with this chapter or the [New York] Convention as ratified by the United States." *Id.* § 208. Chapter 1, in turn, provides that "[a] written provision in . . . a contract evidencing a transaction involving commerce to settle by arbitration a controversy thereafter arising out of such contract or transaction, or the refusal to perform the whole or any part thereof, or an agreement in writing to submit to arbitration an existing controversy arising out of such a contract, transaction, or refusal, shall be valid, irrevocable, and enforceable, save upon such grounds as exist at law or in equity for the revocation of any contract." *Id.* § 2. Chapter 1 further provides that "any party to the arbitration may apply to the court so specified for an order confirming the award, and thereupon the court must grant such an order unless the award is vacated, modified, or corrected as prescribed in sections 10 and 11 of [the FAA]." *Id.* § 9.

Consistent with applicable law, the Department and the Commission will develop a list of at least 10 arbitrators, chosen on the basis of independence, integrity, and expertise. The following shall apply in connection with this process:

Arbitrators:

- (1) will remain on the list for a period of 3 years, absent exceptional circumstances or removal for cause, renewable by the Department, with prior notification to the Commission, for additional 3-year terms;
- (2) shall not be subject to any instructions from, or be affiliated with, either party, or any participating organization, or the U.S., EU, or any EU Member State or any other governmental authority, public authority, or enforcement authority; and
- (3) must be admitted to practice law in the United States and be experts in U.S. privacy law, with expertise in EU data protection law.

G. Arbitration Procedures

The Department and the Commission have agreed, consistent with applicable law, to the adoption of arbitration rules that govern proceedings before the EU-U.S. Data Privacy Framework Panel.²⁰ In the event the rules governing the proceedings need to be changed, the Department and the Commission will agree to amend those rules or adopt a different set of existing, well-established U.S. arbitral procedures, as appropriate, subject to each of the following considerations:

1. An individual may initiate binding arbitration, subject to the pre-arbitration requirements provision above, by delivering a “Notice” to the organization. The Notice shall contain a summary of steps taken under Paragraph C to resolve the claim, a description of the alleged violation, and, at the choice of the individual, any supporting documents and materials and/or a discussion of law relating to the alleged claim.
2. Procedures will be developed to ensure that an individual’s same claimed violation does not receive duplicative remedies or procedures.
3. FTC action may proceed in parallel with arbitration.
4. No representative of the U.S., EU, or any EU Member State or any other governmental authority, public authority, or enforcement authority may participate in these arbitrations, provided, that at the request of an EU individual, DPAs may provide assistance in the preparation only of the Notice but DPAs may not have access to discovery or any other materials related to these arbitrations.
5. The location of the arbitration will be the United States, and the individual may choose video or telephone participation, which will be provided at no cost to the individual. In-person participation will not be required.

²⁰ 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. On September 15, 2017, the Department and the Commission agreed to the adoption of a set of arbitration 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 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.

6. The language of the arbitration will be English unless otherwise agreed by the parties. Upon a reasoned request, and taking into account whether the individual is represented by an attorney, interpretation at the arbitral hearing, as well as translation of arbitral materials will be provided at no cost to the individual, unless the EU-U.S. Data Privacy Framework Panel finds that, under the circumstances of the specific arbitration, this would lead to unjustified or disproportionate costs.
7. Materials submitted to arbitrators will be treated confidentially and will only be used in connection with the arbitration.
8. Individual-specific discovery may be permitted if necessary, and such discovery will be treated confidentially by the parties and will only be used in connection with the arbitration.
9. Arbitrations should be completed within 90 days of the delivery of the Notice to the organization at issue, unless otherwise agreed to by the parties.

H. Costs

Arbitrators should take reasonable steps to minimize the costs or fees of the arbitrations.

The Department will, consistent with applicable law, facilitate the maintenance of a fund, to which participating organizations will be required to contribute, based in part on the size of the organization, which will cover the arbitral cost, including arbitrator fees, up to maximum amounts (“caps”). The fund will be managed by a third party, which will report regularly to the Department on the operations of the fund. The Department will work with the third party to periodically review the operation of the fund, including the need to adjust the amount of the contributions or of the caps 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 participating organizations. The Department will notify the Commission of the outcome of such reviews with the third party and will provide the Commission with prior notification of any adjustments of the amount of the contributions. Attorney’s fees are not covered by this provision or any fund under this provision.



UNITED STATES DEPARTMENT OF COMMERCE
Secretary of Commerce
Washington, D.C. 20230

July 14, 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 United States, I am pleased to transmit herewith a package of the United Kingdom Extension to the EU-U.S. Data Privacy Framework (“UK Extension to the EU-U.S. DPF”) materials that, combined with 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”, reflects important and detailed negotiations to strengthen privacy and civil liberties protections. These negotiations have resulted in new safeguards to ensure that U.S. signals intelligence activities are necessary and proportionate in the pursuit of defined national security objectives and a new mechanism for United Kingdom (“UK”) individuals to seek redress if they believe they are unlawfully targeted by signals intelligence activities, which together will ensure the privacy of UK personal data. The UK Extension to the EU-U.S. DPF will underpin an inclusive and competitive digital economy. We should both be proud of the improvements reflected in that mechanism, which will enhance the protection of privacy around the world. This package, along with the Executive Order, Regulations, and other materials available from public sources, provides a very strong basis for the United Kingdom to grant a data bridge to the United States for the UK Extension to the EU-U.S. DPF.¹

The following materials are attached:

- 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

¹ Under the UK Extension to the EU-U.S. DPF the safeguards, protections, and administration and supervision of the EU-U.S. Data Privacy Framework (“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.

terms under which Data Privacy Framework organizations are obligated to arbitrate certain residual claims as to personal data covered by the Principles);

- A letter from the Department's International Trade Administration, which administers the Data Privacy Framework program, describing the commitments that our Department has made to ensure that the program operates effectively, including as relates to the UK Extension to the EU-U.S. DPF;
- A letter from the Federal Trade Commission describing its enforcement of the Principles, including as relates to the UK Extension to the EU-U.S. DPF;
- A letter from the Department of Transportation describing its enforcement of the Principles, including as relates to the UK Extension to the EU-U.S. DPF; and
- A letter prepared by the Department of Justice regarding safeguards and limitations on U.S. Government access for law enforcement and public interest purposes.

In addition, with respect to references to national security, I refer you to the letter of December 9, 2022 addressed to the Department and prepared by the Office of the Director of National Intelligence regarding safeguards and limitations applicable to U.S. national security authorities. That letter will be available on the Department's Data Privacy Framework website.

Effective as of July 17, 2023 U.S. organizations that wish to self-certify their compliance pursuant to the UK Extension to the EU-U.S. DPF may do so though 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. The full package of materials for the UK Extension to the EU-U.S. DPF will be published on the Department's Data Privacy Framework website together with relevant information with regard to the date of entry into force of the United Kingdom's adequacy regulations and their relevance for personal data received from the United Kingdom in reliance on the UK Extension to the EU-U.S. DPF.

You can be assured that the United States takes these commitments seriously. We look forward to working with you as the UK Extension to the EU-U.S. DPF is implemented and as we embark on the next phase of this process together.

Sincerely,



Gina M. Raimondo



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. law⁴; 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 businesses 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. DPF⁶, 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 arbitration⁹; 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,

A handwritten signature in black ink that reads "Marisa Lago". The signature is written in a cursive, slightly slanted style.

Marisa Lago
Under Secretary for International Trade



UNITED STATES OF AMERICA
Federal Trade Commission
WASHINGTON, D.C. 20580

Office of the Chair

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:

The United States Federal Trade Commission (“FTC”) appreciates the opportunity to address its enforcement role in connection with the EU-U.S. Data Privacy Framework (“EU-U.S. DPF”) Principles as relates to personal data transfers from the United Kingdom. The FTC has long committed to protecting consumers and privacy across borders, and we are committed to enforcement of the commercial sector aspects of this framework. The FTC has performed such a role since the year 2000, in connection with the U.S.-EU Safe Harbor Framework, and most recently since 2016, in connection with the EU-U.S. Privacy Shield Framework.¹ On July 16, 2020, the Court of Justice of the European Union (“CJEU”) invalidated the European Commission’s adequacy decision underlying the EU-U.S. Privacy Shield Framework, on the basis of issues other than the commercial principles that the FTC enforced. The U.S. and the European Commission have since negotiated the EU-U.S. Data Privacy Framework to address that CJEU ruling, and relatedly the United States and the UK Government have since negotiated the United Kingdom Extension to the EU-U.S. Data Privacy Framework (“UK Extension to the EU-U.S. DPF”).

I write to confirm the FTC’s commitment to vigorous enforcement of the EU-U.S. DPF Principles under the UK Extension to the EU-U.S. DPF. Notably, we affirm our commitment in

¹ Letter from Chairwoman Edith Ramirez to Věra Jourová, Commissioner for Justice, Consumers and Gender Equality of the European Commission, Describing Federal Trade Commission Enforcement of the New EU-U.S. Privacy Shield Framework (Feb. 29, 2016), <https://www.ftc.gov/legal-library/browse/cases-proceedings/public-statements/letter-chairwoman-edith-ramirez-vera-jourova-commissioner-justice-consumers-gender-equality-european>. The FTC also previously committed to enforce the U.S.-EU Safe Harbor Program. Letter from Robert Pitofsky, FTC Chairman, to John Mogg, Director DG Internal Market, European Commission (July 14, 2000), <https://www.federalregister.gov/documents/2000/07/24/00-18489/issuance-of-safe-harbor-principles-and-transmission-to-european-commission>. This letter replaces those earlier commitments as relates to personal data transfers from the United Kingdom and Gibraltar.

three key areas: (1) referral prioritization and investigations; (2) seeking and monitoring orders; and (3) enforcement cooperation with the UK Information Commissioner’s Office (“ICO”).²

I. Introduction

a. FTC Privacy Enforcement and Policy Work

The FTC has broad civil enforcement authority to promote consumer protection and competition in the commercial sphere. As part of its consumer protection mandate, the FTC enforces a wide range of laws to protect the privacy and security of consumers and their data. The primary law enforced by the FTC, the FTC Act, prohibits “unfair” or “deceptive” acts or practices in or affecting commerce.³ The FTC also enforces targeted statutes that protect information relating to health, credit, and other financial matters, as well as children’s online information, and has issued regulations implementing each of these statutes.⁴

The FTC has also recently pursued numerous initiatives to strengthen our privacy work. In August of 2022 the FTC announced it is considering rules to crack down on harmful commercial surveillance and lax data security.⁵ The goal of the project is to build a robust public record to inform whether the FTC should issue rules to address commercial surveillance and data security practices, and what those rules should potentially look like.

Our “PrivacyCon” conferences continue to gather leading researchers to discuss the latest research and trends related to consumer privacy and data security. We also have increased our agency’s ability to keep pace with the technology developments at the center of much of our privacy work, building a growing team of technologists and interdisciplinary researchers. In 2014 the FTC and the ICO signed a Memorandum of Understanding, and we have cooperated in numerous public and non-public matters since.⁶ We also recently issued a report to Congress warning about harms associated with using artificial intelligence (“AI”) to address online harms

² The Gibraltar Regulatory Authority (“GRA”) as relates to personal data transfers from Gibraltar.

³ 15 U.S.C. § 45(a). The FTC does not have jurisdiction over criminal law enforcement or national security matters. Nor can the FTC reach most other governmental actions. In addition, there are exceptions to the FTC’s jurisdiction over commercial activities, including with respect to banks, airlines, the business of insurance, and the common carrier activities of telecommunications service providers. The FTC also does not have jurisdiction over most non-profit organizations, though it does have jurisdiction over sham charities or other non-profits that in fact operate for profit. The FTC also has jurisdiction over non-profit organizations that operate for the profit of their for-profit members, including by providing substantial economic benefits to those members. In some instances, the FTC’s jurisdiction is concurrent with that of other law enforcement agencies. We have developed strong working relationships with federal and state authorities, and work closely with them to coordinate investigations or make referrals where appropriate.

⁴ See Privacy and Security, <https://www.ftc.gov/business-guidance/privacy-security>.

⁵ See Press Release, Fed. Trade Comm’n, FTC Explores Rules Cracking Down on Commercial Surveillance and Lax Data Security Practices (Aug. 11, 2022), <https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-explores-rules-cracking-down-commercial-surveillance-lax-data-security-practices>.

⁶ See Press Release, Fed. Trade Comm’n, FTC Signs Memorandum of Understanding with UK Privacy Enforcement Agency (Mar. 6, 2014), <https://www.ftc.gov/news-events/news/press-releases/2014/03/ftc-signs-memorandum-understanding-uk-privacy-enforcement-agency>.

identified by Congress. This report raised concerns regarding inaccuracy, bias, discrimination, and commercial surveillance creep.⁷

b. U.S. Legal Protections Benefitting UK Consumers

The UK Extension to the EU-U.S. DPF operates in the context of the larger U.S. privacy landscape, which also protects UK consumers in a number of ways. The FTC Act’s prohibition on unfair or deceptive acts or practices is not limited to protecting U.S. consumers from U.S. companies, as it includes those practices that (1) cause or are likely to cause reasonably foreseeable injury in the United States, or (2) involve material conduct in the United States. Further, the FTC can use all remedies that are available to protect domestic consumers when protecting foreign consumers.⁸

The FTC also enforces other targeted laws whose protections extend to non-U.S. consumers, such as the Children’s Online Privacy Protection Act (“COPPA”). Among other things, COPPA requires that operators of child-directed websites and online services, or general audience sites that knowingly collect personal information from children under the age of 13, provide parental notice and obtain verifiable parental consent. U.S.-based websites and services that are subject to COPPA and collect personal information from foreign children are required to comply with COPPA. Foreign-based websites and online services must also comply with COPPA if they are directed to children in the United States, or if they knowingly collect personal information from children in the United States. Moreover, in addition to the U.S. federal laws enforced by the FTC, other federal and state consumer protection, data breach, and privacy laws may provide additional benefits to UK consumers.

c. FTC Enforcement Activity

The FTC brought cases under both the U.S.-EU Safe Harbor and EU-U.S. Privacy Shield frameworks and continued to enforce the EU-U.S. Privacy Shield even after the CJEU invalidation of the adequacy decision underlying the EU-U.S. Privacy Shield Framework.⁹ Several of the FTC’s recent complaints have included counts alleging that firms violated EU-U.S. Privacy Shield provisions, including in proceedings against Twitter,¹⁰ CafePress,¹¹ and

⁷ See Press Release, Fed. Trade Comm’n, FTC Report Warns About Using Artificial Intelligence to Combat Online Problems (June 16, 2022), <https://www.ftc.gov/news-events/news/press-releases/2022/06/ftc-report-warns-about-using-artificial-intelligence-combat-online-problems>.

⁸ 15 U.S.C. § 45(a)(4)(B). Further, “unfair or deceptive acts or practices” includes such acts or practices involving foreign commerce that (i) cause or are likely to cause reasonably foreseeable injury within the United States; or (ii) involve material conduct occurring within the United States. 15 U.S.C. § 45(a)(4)(A).

⁹ See Appendix A for a list of FTC Safe Harbor and Privacy Shield matters.

¹⁰ See Press Release, Fed. Trade Comm’n, FTC Charges Twitter with Deceptively Using Account Security Data to Sell Targeted Ads (May 25, 2022), <https://www.ftc.gov/news-events/news/press-releases/2022/05/ftc-charges-twitter-deceptively-using-account-security-data-sell-targeted-ads>.

¹¹ See Press Release, Fed. Trade Comm’n, FTC Takes Action Against CafePress for Data Breach Cover Up (Mar., 2022), <https://www.ftc.gov/news-events/news/press-releases/2022/03/ftc-takes-action-against-cafepress-data-breach-cover>.

Flo.¹² In the enforcement action against Twitter, the FTC secured \$150 million from Twitter for its violation of an earlier FTC order with practices affecting more than 140 million customers, including violating EU-U.S. Privacy Shield Principle 5 (Data Integrity and Purpose Limitation). Further, the agency's order requires that Twitter allow users to employ secure multi-factor authentication methods that do not require users to provide their telephone numbers.

In *CafePress*, the FTC alleged that the company failed to secure consumers' sensitive information, covered up a major data breach, and violated EU-U.S. Privacy Shield Principles 2 (Choice), 4 (Security), and 6 (Access). The FTC's order requires the company to replace inadequate authentication measures with multifactor authentication, substantively limit the amount of data it collects and retains, encrypt Social Security numbers, and have a third party assess its information security programs and provide the FTC with a copy that can be publicized.

In *Flo*, the FTC alleged that the fertility-tracking app disclosed user health information to third-party data analytics providers after commitments to keep such information private. The FTC complaint specifically notes the company's interactions with EU consumers and that Flo violated EU-U.S. Privacy Shield Principles 1 (Notice), 2 (Choice), 3 (Accountability for Onward Transfer), and 5 (Data Integrity and Purpose Limitation). Among other things, the agency's order requires Flo to notify affected users about the disclosure of their personal information and to instruct any third party that received users' health information to destroy that data. Importantly, FTC orders protect all consumers worldwide who interact with a U.S. business, not just those consumers who have lodged complaints.

Many past U.S.-EU Safe Harbor and EU-U.S. Privacy Shield enforcement cases involved organizations that completed an initial self-certification through the Department of Commerce, but failed to maintain their annual self-certification while they continued to represent themselves as current participants. Other cases involved false claims of participation by organizations that never completed an initial self-certification through the Department of Commerce. Going forward, we expect to focus our proactive enforcement efforts on the types of substantive violations of the EU-U.S. DPF Principles alleged in cases such as Twitter, CafePress, and Flo. Meanwhile, the Department of Commerce will administer and supervise the self-certification process, maintain the authoritative list of EU-U.S. DPF and, as applicable, UK Extension to the EU-U.S. DPF participants, and address other program participation claim issues.¹³ Importantly, organizations claiming EU-U.S. DPF and, as applicable, UK Extension to the EU-U.S. DPF participation may be subject to substantive enforcement of the EU-U.S. DPF Principles even if they fail to make or maintain their self-certification through the Department of Commerce.

II. Referral Prioritization and Investigations

¹² See Press Release, Fed. Trade Comm'n, FTC Finalizes Order with Flo Health, a Fertility-Tracking App that Shared Sensitive Health Data with Facebook, Google, and Others (June 22, 2021), <https://www.ftc.gov/news-events/news/press-releases/2021/06/ftc-finalizes-order-flo-health-fertility-tracking-app-shared-sensitive-health-data-facebook-google>.

¹³ Letter from Marisa Lago, Under Secretary of Commerce for International Trade, to the Right Honorable Chloe Smith MP, Secretary of State, Department of Science, Innovation and Technology (DSIT) (July 13, 2023).

As we did under the U.S.-EU Safe Harbor Framework and the EU-U.S. Privacy Shield Framework, the FTC commits to give priority consideration to EU-U.S. DPF Principles referrals from the Department of Commerce, EU data protection authorities (“DPAs”), and the ICO. We will also prioritize consideration of referrals for non-compliance with the EU-U.S. DPF Principles from privacy self-regulatory organizations and other independent dispute resolution bodies.

To facilitate referrals under the UK Extension to the EU-U.S. DPF from the ICO, the FTC has created a standardized referral process and has provided guidance to the ICO on the type of information that would best assist the FTC in its inquiry into a referral. As part of this effort, the FTC has designated an agency point of contact for ICO referrals. It is most useful when the ICO has conducted a preliminary inquiry into the alleged violation and can cooperate with the FTC in an investigation.

Upon receipt of such a referral from the Department of Commerce, the ICO, or self-regulatory organization or other independent dispute resolution bodies the FTC can take a range of actions to address the issues raised. For example, we may review the organization’s privacy policies, obtain further information directly from the organization or from third parties, follow up with the referring entity, assess whether there is a pattern of violations or significant number of consumers affected, determine whether the referral implicates issues within the purview of the Department of Commerce, assess whether additional efforts to put market participants on notice would be helpful, and, as appropriate, initiate an enforcement proceeding.

In addition to prioritizing EU-U.S. DPF Principles referrals from the Department of Commerce, the ICO, and privacy self-regulatory organizations or other independent dispute resolution bodies,¹⁴ the FTC will continue to investigate significant EU-U.S. DPF Principles violations on its own initiative where appropriate, using a range of tools. As part of the FTC’s program of investigating privacy and security issues involving commercial organizations, the agency has routinely examined whether the entity at issue was making EU-U.S. Privacy Shield representations. If the entity made such representations and the investigation revealed apparent violations of the EU-U.S. Privacy Shield Principles, the FTC included allegations of EU-U.S. Privacy Shield violations in its enforcement actions. We will continue this proactive approach, now with respect to the EU-U.S. DPF Principles.

III. Seeking and Monitoring Orders

The FTC also affirms its commitment to seek and monitor enforcement orders to ensure compliance with the EU-U.S. DPF Principles. We will require compliance with the EU-U.S. DPF Principles through a variety of appropriate injunctive provisions in future FTC EU-U.S. DPF Principles orders. Violations of the FTC’s administrative orders can lead to civil penalties

¹⁴ Although the FTC does not resolve or mediate individual consumer complaints, the FTC affirms that it will prioritize EU-U.S. DPF Principles referrals from the ICO. In addition, the FTC uses complaints in its Consumer Sentinel database, which is accessible by many other law enforcement agencies, to identify trends, determine enforcement priorities, and identify potential investigative targets. UK individuals can use the same complaint system available to U.S. consumers to submit a complaint to the FTC at <https://reportfraud.ftc.gov/>. For individual EU-U.S. DPF Principles complaints, however, it may be most useful for UK individuals to submit complaints to the ICO and/or, as applicable, the GRA or independent dispute resolution body.

of up to \$ 50,120 per violation, or \$50,120 per day for a continuing violation,¹⁵ which, in the case of practices affecting many consumers, can amount to millions of dollars. Each consent order also has reporting and compliance provisions. The entities under order must retain documents demonstrating their compliance for a specified number of years. The orders must also be disseminated to employees responsible for ensuring order compliance.

The FTC systematically monitors compliance with existing EU-U.S. Privacy Shield Principles orders, as it does with all of its orders, and brings actions to enforce them when necessary.¹⁶ Importantly, FTC orders will continue to protect all consumers worldwide who interact with a business, not just those consumers who have lodged complaints. Finally, the FTC will maintain an online list of companies subject to orders obtained in connection with enforcement of the EU-U.S. DPF Principles.¹⁷

IV. Enforcement Cooperation with the ICO

The FTC recognizes the important role that the ICO can play with respect to EU-U.S. DPF Principles compliance and encourages increased consultation and enforcement cooperation. Indeed, a coordinated approach to the challenges posed by current digital market developments, and data-intensive business models, is increasingly critical. The FTC will exchange information on referrals with referring enforcement authorities, including the status of referrals, subject to confidentiality laws and restrictions. To the extent feasible given the number and type of referrals received, the information provided will include an evaluation of the referred matters, including a description of significant issues raised and any action taken to address law violations within the jurisdiction of the FTC. The FTC will also provide feedback to the referring authority on the types of referrals received in order to increase the effectiveness of efforts to address unlawful conduct. If a referring enforcement authority seeks information about the status of a particular referral for purposes of pursuing its own enforcement proceeding, the FTC will respond, taking into account the number of referrals under consideration and subject to confidentiality and other legal requirements.

The FTC will also work closely with the ICO to provide enforcement assistance. In appropriate cases, this could include information sharing and investigative assistance pursuant to the U.S. SAFE WEB Act, which authorizes FTC assistance to foreign law enforcement agencies when the foreign agency is enforcing laws prohibiting practices that are substantially similar to those prohibited by laws the FTC enforces.¹⁸ As part of this assistance, the FTC can share information obtained in connection with an FTC investigation, issue compulsory process on

¹⁵ 15 U.S.C. § 45(m); 16 C.F.R. § 1.98. This amount is periodically adjusted for inflation.

¹⁶ Last year the FTC voted to streamline the process for investigating repeat offenders. *See* Press Release, Fed. Trade Comm'n, FTC Authorizes Investigations into Key Enforcement Priorities (Jul. 1, 2021), <https://www.ftc.gov/news-events/news/press-releases/2021/07/ftc-authorizes-investigations-key-enforcement-priorities>.

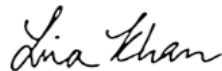
¹⁷ *Cf.* Privacy Shield, <https://www.ftc.gov/business-guidance/privacy-security/privacy-shield>.

¹⁸ In determining whether to exercise its U.S. SAFE WEB Act authority, the FTC considers, inter alia: “(A) whether the requesting agency has agreed to provide or will provide reciprocal assistance to the Commission; (B) whether compliance with the request would prejudice the public interest of the United States; and (C) whether the requesting agency’s investigation or enforcement proceeding concerns acts or practices that cause or are likely to cause injury to a significant number of persons.” 15 U.S.C. § 46(j)(3). This authority does not apply to enforcement of competition laws.

behalf of the ICO conducting its own investigation, and seek oral testimony from witnesses or defendants in connection with the ICO's enforcement proceeding, subject to the requirements of the U.S. SAFE WEB Act. The FTC regularly uses this authority to assist other authorities around the world in privacy and consumer protection cases.

In addition to any consultation with the ICO on case-specific matters, the FTC will participate in periodic meetings with the ICO to discuss in general terms how to improve enforcement cooperation. The FTC will also participate, along with the Department of Commerce, DSIT, and ICO and GRA representatives, as appropriate, in periodic discussions on the UK Extension to the EU-U.S. DPF to discuss its implementation. The FTC also encourages the development of tools that will enhance enforcement cooperation with the ICO, as well as other privacy enforcement authorities around the world. The FTC is pleased to affirm its commitment to enforcing the commercial sector aspects of the UK Extension to the EU-U.S. DPF. We see our partnership with UK colleagues as a critical part of providing privacy protection for both our citizens and yours.

Sincerely,

A handwritten signature in black ink that reads "Lina Khan". The signature is written in a cursive, flowing style.

Lina M. Khan
Chair, Federal Trade Commission

Appendix A
Privacy Shield and Safe Harbor Enforcement

	Docket/FTC File No.	Case	Link
1	FTC File No. 2023062 Case No. 3:22-cv-03070 (N.D. Cal.)	US v. Twitter, Inc.	Twitter
2	FTC File No. 192 3209	In the Matter of Residual Pumpkin Entity, LLC, formerly d/b/a CafePress , and PlanetArt, LLC, d/b/a CafePress	CafePress
3	FTC File No. 192 3133 Docket No. C-4747	In the Matter of Flo Health, Inc.	Flo Health
4	FTC File No. 192 3050 Docket No. C-4723	In the Matter of Ortho-Clinical Diagnostics, Inc.	Ortho-Clinical
5	FTC File No. 192 3092 Docket No. C-4709	In the Matter of T&M Protection, LLC	T&M Protection
6	FTC File No. 192 3084 Docket No. C-4704	In the Matter of TDARX, Inc.	TDARX
7	FTC File No. 192 3093 Docket No. C-4706	In the Matter of Global Data Vault, LLC	Global Data
8	FTC File No. 192 3078 Docket No. C-4703	In the Matter of Incentive Services, Inc.	Incentive Services
9	FTC File No. 192 3090 Docket No. C-4705	In the Matter of Click Labs, Inc.	Click Labs
10	FTC File No. 182 3192 Docket No. C-4697	In the Matter of Medable, Inc.	Medable
11	FTC File No. 182 3189 Docket No. 9386	In the Matter of NTT Global Data Centers Americas, Inc., as successor in interest to RagingWire Data Centers, Inc.	RagingWire
12	FTC File No. 182 3196 Docket No. C-4702	In the Matter of Thru, Inc.	Thru
13	FTC File No. 182 3188 Docket No. C-4698	In the Matter of DCR Workforce, Inc.	DCR Workforce
14	FTC File No. 182 3194 Docket No. C-4700	In the Matter of LotaData, Inc.	LotaData
15	FTC File No. 182 3195 Docket No. C-4701	In the Matter of EmpiriStat, Inc.	EmpiriStat
16	FTC File No. 182 3193 Docket No. C-4699	In the Matter of 214 Technologies, Inc., also d/b/a Trueface.ai	Trueface.ai

17	FTC File No. 182 3107 Docket No. 9383	In the Matter of Cambridge Analytica, LLC	Cambridge Analytica
18	FTC File No. 182 3152 Docket No. C-4685	In the Matter of SecureTest, Inc.	SecureTest
19	FTC File No. 182 3144 Docket No. C-4664	In the Matter of VenPath, Inc.	VenPath
20	FTC File No. 182 3154 Docket No. C-4666	In the Matter of SmartStart Employment Screening, Inc.	SmartStart
21	FTC File No. 182 3143 Docket No. C-4663	In the Matter of mResourceLLC , d/b/a Loop Works LLC	mResource
22	FTC File No. 182 3150 Docket No. C-4665	In the Matter of IDmission LLC	IDmission
23	FTC File No. 182 3100 Docket No. C-4659	In the Matter of ReadyTech Corporation	ReadyTech
24	FTC File No. 172 3173 Docket No. C-4630	In the Matter of Decusoft, LLC	Decusoft
25	FTC File No. 172 3171 Docket No. C-4628	In the Matter of Tru Communication, Inc.	Tru
26	FTC File No. 172 3172 Docket No. C-4629	In the Matter of Md7, LLC	Md7
30	FTC File No. 152 3198 Docket No. C-4543	In the Matter of Jhayrmaine Daniels (d/b/a California Skate-Line)	Jhayrmaine Daniels
31	FTC File No. 152 3190 Docket No. C-4545	In the Matter of Dale Jarrett Racing Adventure, Inc.	Dale Jarrett
32	FTC File No. 152 3141 Docket No. C-4540	In the Matter of Golf Connect, LLC	Golf Connect
33	FTC File No. 152 3202 Docket No. C-4546	In the Matter of Inbox Group, LLC	Inbox Group
34	File No. 152 3187 Docket No. C-4542	In the Matter of IOActive, Inc.	IOActive
35	FTC File No. 152 3140 Docket No. C-4549	In the Matter of Jubilant Clinsys, Inc.	Jubilant
36	FTC File No. 152 3199 Docket No. C-4547	In the Matter of Just Bagels Manufacturing, Inc.	Just Bagels
37	FTC File No. 152 3138 Docket No. C-4548	In the Matter of NAICS Association, LLC	NAICS
38	FTC File No. 152 3201 Docket No. C-4544	In the Matter of One Industries Corp.	One Industries
39	FTC File No. 152 3137 Docket No. C-4550	In the Matter of Pinger, Inc.	Pinger

40	FTC File No. 152 3193 Docket No. C-4552	In the Matter of SteriMed Medical Waste Solutions	SteriMed
41	FTC File No. 152 3184 Docket No. C-4541	In the Matter of Contract Logix, LLC	Contract Logix
42	FTC File No. 152 3185 Docket No. C-4551	In the Matter of Forensics Consulting Solutions, LLC	Forensics Consulting
43	FTC File No. 152 3051 Docket No. C-4526	In the Matter of American Int'l Mailing, Inc.	AIM
44	FTC File No. 152 3015 Docket No. C-4525	In the Matter of TES Franchising, LLC	TES
45	FTC File No. 142 3036 Docket No. C-4459	In the Matter of American Apparel, Inc.	American Apparel
46	FTC File No. 142 3026 Docket No. C-4469	In the Matter of Fantage.com, Inc.	Fantage
47	FTC File No. 142 3017 Docket No. C-4461	In the Matter of Apperian, Inc.	Apperian
48	FTC File No. 142 3018 Docket No. C-4462	In the Matter of Atlanta Falcons Football Club, LLC	Atlanta Falcons
49	FTC File No. 142 3019 Docket No. C-4463	In the Matter of Baker Tilly Virchow Krause, LLP	Baker Tilly
50	FTC File No. 142 3020 Docket No. C-4464	In the Matter of BitTorrent, Inc.	BitTorrent
51	FTC File No. 142 3022 Docket No. C-4465	In the Matter of Charles River Laboratories, Int'l	Charles River
52	FTC File No. 142 3023 Docket No. C-4466	In the Matter of DataMotion, Inc.	DataMotion
53	FTC File No. 142 3024 Docket No. C-4467	In the Matter of DDC Laboratories, Inc., d/b/a DNA Diagnostics Center	DDC
54	FTC File No. 142 3028 Docket No. C-4470	In the Matter of Level 3 Communications, LLC	Level 3
55	FTC File No. 142 3025 Docket No. C-4468	In the Matter of PDB Sports, Ltd., d/b/a the Denver Broncos Football Club, LLP	Broncos
56	FTC File No. 142 3030 Docket No. C-4471	In the Matter of Reynolds Consumer Products, Inc.	Reynolds
57	FTC File No. 142 3031 Docket No. C-4472	In the Matter of Receivable Management Services Corporation	Receivable Mgmt
58	FTC File No. 142 3032 Docket No. C-4473	In the Matter of Tennessee Football, Inc.	Tennessee Football
59	FTC File No. 102 3058 Docket No. C-4369	In the Matter of Myspace LLC	Myspace

60	FTC File No. 092 3184 Docket No. C-4365	In the Matter of Facebook, Inc.	Facebook
61	FTC File No. 092 3081 Civil Action No. 09-CV- 5276 (C.D. Cal.)	FTC v. Javian Karnani, and Balls of Kryptonite, LLC , d/b/a Bite Size Deals, LLC, and Best Priced Brands, LLC	Balls of Kryptonite
62	FTC File No. 102 3136 Docket No. C-4336	In the Matter of Google, Inc.	Google
63	FTC File No. 092 3137 Docket No. C-4282	In the Matter of World Innovators, Inc.	World Innovators
64	FTC File No. 092 3141 Docket No. C-4271	In the Matter of Progressive Gaitways LLC	Progressive Gaitways
65	FTC File No. 092 3139 Docket No. C-4270	In the Matter of Onyx Graphics, Inc.	Onyx Graphics
66	FTC File No. 092 3138 Docket No. C-4269	In the Matter of ExpatEdge Partners, LLC	ExpatEdge
67	FTC File No. 092 3140 Docket No. C-4281	In the Matter of Directors Desk LLC	Directors Desk
68	FTC File No. 092 3142 Docket No. C-4272	In the Matter of Collectify LLC	Collectify



THE SECRETARY OF TRANSPORTATION
WASHINGTON, DC 20590

July 14, 2023

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

Dear Acting Secretary of State Smith:

The United States Department of Transportation (“Department” or “DOT”) appreciates the opportunity to describe its role in enforcing the EU-U.S. Data Privacy Framework (“EU-U.S. DPF”) Principles as relates to personal data transfers from the United Kingdom. The EU-U.S. DPF Principles will play a critical role in protecting personal data provided during commercial transactions in an increasingly interconnected world. It will enable businesses to conduct important operations in the global economy, while at the same time ensuring that UK consumers retain important privacy protections.

The DOT first publicly expressed its commitment to enforcement of the U.S.-EU Safe Harbor Framework in a letter sent to the European Commission over 22 years ago, commitments that were repeated and expanded upon in a 2016 letter regarding the EU-U.S. Privacy Shield Framework. The DOT pledged to vigorously enforce the U.S.-EU Safe Harbor Privacy Principles, and then the EU-U.S. Privacy Shield Principles, in those letters. The DOT extends this commitment to the EU-U.S. DPF Principles under the United Kingdom Extension to the EU-U.S. Data Privacy Framework (“UK Extension to the EU-U.S. DPF”) and this letter memorializes that commitment.¹

Notably, the DOT confirms its commitment to enforcement of the EU-U.S. DPF Principles under the UK Extension to the EU-U.S. DPF in the following key areas: (1) prioritizing investigation of alleged EU-U.S. DPF Principles violations; (2) appropriate enforcement action against entities making false or deceptive claims of UK Extension to the EU-U.S. DPF participation; and (3) monitoring and making public enforcement orders concerning EU-U.S. DPF Principles violations. We provide information about each of these commitments and, for necessary context, pertinent background about the DOT’s role in protecting consumer privacy and enforcing the EU-U.S. DPF Principles.

¹ This letter memorializes that commitment as relates to personal data transfers from the United Kingdom and, as applicable, Gibraltar.

I. Background

A. DOT's Privacy Authority

The Department is strongly committed to ensuring the privacy of information provided by consumers to airlines and ticket agents. The DOT's authority to take action in this area is found in 49 U.S.C. 41712, which prohibits a carrier or ticket agent from engaging in "an unfair or deceptive practice" in air transportation or the sale of air transportation. Section 41712 is patterned after Section 5 of the Federal Trade Commission (FTC) Act (15 U.S.C. 45). Recently, DOT issued regulations defining unfair and deceptive practices, consistent with both DOT and FTC precedent (14 CFR § 399.79). Specifically, a practice is "unfair" if it causes or is likely to cause substantial injury, which is not reasonably avoidable, and the harm is not outweighed by benefits to consumers or competition. A practice is "deceptive" to consumers if it is likely to mislead a consumer, acting reasonably under the circumstances, with respect to a material matter. A matter is material if it is likely to have affected the consumer's conduct or decision with respect to a product or service. Aside from these general principles, DOT specifically interprets section 41712 as prohibiting carriers and ticket agents from: (1) violating the terms of its privacy policy; (2) violating any rule issued by the Department that identifies specific privacy practices as unfair or deceptive; or (3) violating the Children's Online Privacy Protection Act (COPPA) or FTC rules implementing COPPA; or (4) failing, as a participant in the EU-U.S. DPF and, as applicable, the UK Extension to the EU-U.S. DPF, to comply with the EU-U.S. DPF Principles.²

As noted above, under federal law, the DOT has exclusive authority to regulate the privacy practices of airlines, and it shares jurisdiction with the FTC with respect to the privacy practices of ticket agents in the sale of air transportation.

As such, once a carrier or seller of air transportation publicly commits to the EU-U.S. DPF Principles, the Department is able to use the statutory powers of section 41712 to ensure compliance with those principles. Therefore, once a passenger provides information to a carrier or ticket agent that has committed to honoring the EU-U.S. DPF Principles, any failure to do so by the carrier or ticket agent would be a violation of section 41712.

B. Enforcement Practices

The Department's Office of Aviation Consumer Protection ("OACP")³ investigates and prosecutes cases under 49 U.S.C. 41712. It enforces the statutory prohibition in section 41712 against unfair and deceptive practices primarily through negotiation, preparing cease and desist orders, and drafting orders assessing civil penalties. The office learns of potential violations largely from complaints it receives from individuals, travel agents, airlines, and U.S. and foreign government agencies. Consumers may use the DOT's website to file privacy complaints against airlines and ticket agents.⁴

² <https://www.transportation.gov/individuals/aviation-consumer-protection/privacy>.

³ Formerly known as the Office of Aviation Enforcement and Proceedings.

⁴ <http://www.transportation.gov/airconsumer/privacy-complaints>.

If a reasonable and appropriate settlement in a case is not reached, OACP has the authority to institute an enforcement proceeding involving an evidentiary hearing before a DOT administrative law judge (“ALJ”). The ALJ has the authority to issue cease-and-desist orders and civil penalties. Violations of section 41712 can result in the issuance of cease and desist orders and the imposition of civil penalties of up to \$37,377 for each violation of section 41712.

The Department does not have the authority to award damages or provide pecuniary relief to individual complainants. However, the Department does have the authority to approve settlements resulting from investigations brought by its OACP that directly benefit consumers (e.g., cash, vouchers) as an offset to monetary penalties otherwise payable to the U.S. Government. This has occurred in the past, and may also occur in the context of the EU-U.S. DPF Principles when circumstances warrant. Repeated violations of section 41712 by an airline would also raise questions regarding the airline’s compliance disposition which could, in egregious situations, result in an airline being found to be no longer fit to operate and, therefore, losing its economic operating authority.

To date, the DOT has received relatively few complaints involving alleged privacy violations by ticket agents or airlines. When they arise, they are investigated according to the principles set forth above.

C. DOT Legal Protections Benefiting UK Consumers

Under section 41712, the prohibition on unfair or deceptive practices in air transportation or the sale of air transportation applies to U.S. and foreign air carriers as well as ticket agents. The DOT frequently takes action against U.S. and foreign airlines for practices that affect both foreign and U.S. consumers on the basis that the airline’s practices took place in the course of providing transportation to or from the United States. The DOT does and will continue to use all remedies that are available to protect both foreign and U.S. consumers from unfair or deceptive practices in air transportation by regulated entities.

The DOT also enforces, with respect to airlines, other targeted laws whose protections extend to non-U.S. consumers such as the Children’s Online Privacy Act (“COPPA”). Among other things, COPPA requires that operators of child-directed websites and online services, or general audience sites that knowingly collect personal information from children under 13 provide parental notice and obtain verifiable parental consent. U.S.-based websites and services that are subject to COPPA and collect personal information from foreign children are required to comply with COPPA. Foreign-based websites and online services must also comply with COPPA if they are directed to children in the United States, or if they knowingly collect personal information from children in the United States. To the extent that U.S. or foreign airlines doing business in the United States violate COPPA, the DOT would have jurisdiction to take enforcement action.

II. **EU-U.S. DPF Principles Enforcement**

If an airline or ticket agent chooses to participate in the EU-U.S. DPF and, as applicable, the UK Extension to the EU-U.S. DPF and the Department receives a complaint that such an airline or

ticket agent had allegedly violated the EU-U.S. DPF Principles, the Department would take the following steps to vigorously enforce the EU-U.S. DPF Principles.

A. Prioritizing Investigation of Alleged EU-U.S. DPF Principles Violations

The Department's OACP will investigate each complaint alleging EU-U.S. DPF Principles violations, including complaints received from the UK Information Commissioner's Office ("ICO")⁵ and take enforcement action where there is evidence of a violation. Further, OACP will cooperate with the FTC and Department of Commerce and place a priority on allegations that the regulated entities are not complying with privacy commitments made as part of the UK Extension to the EU-U.S. DPF.

Upon receipt of an allegation of a violation of the EU-U.S. DPF Principles, OACP may take a range of actions as part of its investigation. For example, it may review the ticket agent or airline's privacy policies, obtain further information from the ticket agent or airline or from third parties, follow up with the referring entity, and assess whether there is a pattern of violations or significant number of consumers affected. In addition, it would determine whether the issue implicates matters within the purview of the Department of Commerce or FTC, assess whether consumer education and business education would be helpful, and as appropriate, initiate an enforcement proceeding.

If the Department becomes aware of potential EU-U.S. DPF Principles violations by ticket agents, it will coordinate with the FTC on the matter. We will also advise the FTC and the Department of Commerce of the outcome of any EU-U.S. DPF Principles enforcement action.

B. Addressing False or Deceptive Participation Claims Concerning UK Extension to the EU-U.S. DPF

The Department remains committed to investigating EU-U.S. DPF Principles violations, including false or deceptive claims of participation in the EU-U.S. DPF and, as applicable, the UK Extension to the EU-U.S. DPF. We will give priority consideration to referrals from the Department of Commerce regarding organizations that it identifies as improperly holding themselves out to be EU-U.S. DPF and, as applicable, UK Extension to the EU-U.S. DPF participants or using the EU-U.S. DPF certification mark without authorization.

In addition, we note that if an organization's privacy policy promises that it complies with the EU-U.S. DPF Principles, its failure to make or maintain a self-certification through the Department of Commerce likely will not, by itself, excuse the organization from DOT enforcement of those commitments.

C. Monitoring and Making Public Enforcement Orders Concerning EU-U.S. DPF Principles Violations

⁵ The Gibraltar Regulatory Authority ("GRA") as relates to personal data transfers from Gibraltar.

The Right Honorable Chloe Smith

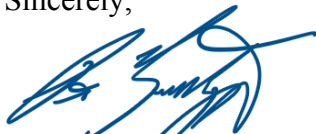
Page 5

The Department's OACP also remains committed to monitoring enforcement orders as needed to ensure compliance with the EU-U.S. DPF Principles. Specifically, if the office issues an order directing an airline or ticket agent to cease and desist from future violations of the EU-U.S. DPF Principles and section 41712, it will monitor the entity's compliance with the cease-and-desist provision in the order. In addition, the office will ensure that orders resulting from EU-U.S. DPF Principles cases are available on its website.

We look forward to our continued work with our federal partners and UK stakeholders on UK Extension to the EU-U.S. DPF matters.

I hope that this information proves helpful. If you have any questions or need further information, please feel free to contact me.

Sincerely,

A handwritten signature in blue ink, appearing to read "Pete Buttigieg", with a stylized flourish extending from the end.

Pete Buttigieg



U.S. Department of Justice

Criminal Division

Office of Assistant Attorney General

Washington, D.C. 20530

July 14, 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:

This letter provides a brief overview of the primary investigative tools used to obtain commercial data and other record information from corporations in the United States for criminal law enforcement or public interest (civil and regulatory) purposes, including the access limitations set forth in those authorities.¹ All the legal processes described in this letter are nondiscriminatory in that they are used to obtain information from corporations in the United States, including from companies that will self-certify through the United Kingdom Extension to the EU-U.S. Data Privacy Framework ("UK Extension to the EU-U.S. DPF"), without regard to the nationality or place of residence of the data subject. Further, corporations that receive legal process in the United States may challenge it in court as discussed below.²

Of particular note with respect to the seizure of data by public authorities is the Fourth Amendment to the United States Constitution, which provides that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported

¹ This overview does not describe the national security investigative tools used by law enforcement in terrorism and other national security investigations, including National Security Letters (NSLs) for certain record information in credit reports, financial records, and electronic subscriber and transaction records, 12 U.S.C. § 3414; 15 U.S.C. § 1681u; 15 U.S.C. § 1681v; 18 U.S.C. § 2709, 50 U.S.C. § 3162, and for electronic surveillance, search warrants, business records, and other collection of information pursuant to the Foreign Intelligence Surveillance Act, 50 U.S.C. § 1801 et seq.

² This letter discusses federal law enforcement and regulatory authorities. Violations of state law are investigated by state law enforcement authorities and are tried in state courts. State law enforcement authorities use warrants and subpoenas issued under state law in essentially the same manner as described herein, but with the possibility that state legal process may be subject to additional protections provided by state constitutions or statutes that exceed those of the U.S. Constitution. State law protections must be at least equal to those of the U.S. Constitution, including but not limited to the Fourth Amendment.

by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.” U.S. Const. amend. IV. As the United States Supreme Court stated in *Berger v. State of New York*, “[t]he basic purpose of this Amendment, as recognized in countless decisions of this Court, is to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials.” 388 U.S. 41, 53 (1967) (citing *Camara v. Mun. Court of San Francisco*, 387 U.S. 523, 528 (1967)). In domestic criminal investigations, the Fourth Amendment generally requires law enforcement officers to obtain a court-issued warrant before conducting a search. See *Katz v. United States*, 389 U.S. 347, 357 (1967). Standards for the issuance of a warrant, such as the probable cause and particularity requirements, apply to warrants for physical searches and seizures as well as to warrants for the stored content of electronic communications issued under the Stored Communications Act as discussed below. When the warrant requirement does not apply, government activity is still subject to a “reasonableness” test under the Fourth Amendment. The Constitution itself, therefore, ensures that the U.S. government does not have limitless, or arbitrary, power to seize private information.³

Criminal Law Enforcement Authorities:

Federal prosecutors, who are officials of the Department of Justice (DOJ), and federal investigative agents including agents of the Federal Bureau of Investigation (FBI), a law enforcement agency within DOJ, are able to compel production of documents and other record information from corporations in the United States for criminal investigative purposes through several types of compulsory legal processes, including grand jury subpoenas, administrative subpoenas, and search warrants, and may acquire other communications pursuant to federal criminal wiretap and pen register authorities.

Grand Jury or Trial Subpoenas: Criminal subpoenas are used to support targeted law enforcement investigations. A grand jury subpoena is an official request issued from a grand jury (usually at the request of a federal prosecutor) to support a grand jury investigation into a particular suspected violation of criminal law. Grand juries are an investigative arm of the court and are empaneled by a judge or magistrate. A subpoena may require someone to testify at a proceeding, or to produce or make available business records, electronically stored information, or other tangible items. The information must be relevant to the investigation and the subpoena cannot be unreasonable because it is overbroad, or because it is oppressive or burdensome. A recipient can file a motion to challenge a subpoena based on those grounds. See Fed. R. Crim. P. 17. In limited circumstances, trial subpoenas for documents may be used after the case has been indicted by the grand jury.

Administrative Subpoena Authority: Administrative subpoena authorities may be exercised in criminal or civil investigations. In the criminal law enforcement context, several federal statutes authorize the use of administrative subpoenas to produce or make available business records, electronically stored information, or other tangible items relevant to

³ With respect to the Fourth Amendment principles on safeguarding privacy and security interests that are discussed above, U.S. courts regularly apply those principles to new types of law enforcement investigative tools that are enabled by developments in technology. For example, in 2018 the Supreme Court ruled that the government’s acquisition in a law enforcement investigation of historical cell-site location information from a cell phone company for an extended period of time is a “search” subject to the Fourth Amendment warrant requirement. *Carpenter v. United States*, 138 S. Ct. 2206 (2018).

investigations involving health care fraud, child abuse, Secret Service protection, controlled substance cases, and Inspector General investigations implicating government agencies. If the government seeks to enforce an administrative subpoena in court, the recipient of the administrative subpoena, like the recipient of a grand jury subpoena, can argue that the subpoena is unreasonable because it is overbroad, or because it is oppressive or burdensome.

Court Orders For Pen Register and Trap and Traces: Under criminal pen register and trap-and-trace provisions, law enforcement may obtain a court order to acquire real-time, non-content dialing, routing, addressing, and signaling information about a phone number or email upon certification that the information provided is relevant to a pending criminal investigation. See 18 U.S.C. §§ 3121-3127. The use or installation of such a device outside the law is a federal crime.

Electronic Communications Privacy Act (ECPA): Additional rules govern the government's access to subscriber information, traffic data, and stored content of communications held by internet service providers (also known as "ISPs"), telephone companies, and other third-party service providers, pursuant to Title II of ECPA, also called the Stored Communications Act (SCA), 18 U.S.C. §§ 2701-2712. The SCA sets forth a system of statutory privacy rights that limit law enforcement access to data beyond what is required under Constitutional law from customers and subscribers of ISPs. The SCA provides for increasing levels of privacy protections depending on the intrusiveness of the collection. For subscriber registration information, Internet Protocol (IP) addresses and associated time stamps, and billing information, criminal law enforcement authorities must obtain a subpoena. For most other stored, non-content information, such as email headers without the subject line, law enforcement must present specific facts to a judge demonstrating that the requested information is relevant and material to an ongoing criminal investigation. To obtain the stored content of electronic communications, generally, criminal law enforcement authorities must obtain a warrant from a judge based on probable cause to believe the account in question contains evidence of a crime. The SCA also provides for civil liability and criminal penalties.⁴

Court Orders for Surveillance Pursuant to Federal Wiretap Law: Additionally, law enforcement may intercept in real time wire, oral, or electronic communications for criminal investigative purposes pursuant to the federal wiretap law. See 18 U.S.C. §§ 2510-2523. This authority is available only pursuant to a court order in which a judge finds, inter alia, that there is probable cause to believe that the wiretap or electronic interception will produce evidence of a federal crime, or the whereabouts of a fugitive fleeing from prosecution. The statute provides for civil liability and criminal penalties for violations of the wiretapping provisions.

Search Warrant—Fed. R. Crim. P. Rule 41: Law enforcement can physically search premises in the United States when authorized to do so by a judge. Law enforcement must

⁴ In addition, section 2705(b) of the SCA authorizes the government to obtain a court order, based on a demonstrated need for protection from disclosure, prohibiting a communications services provider from voluntarily notifying its users of the receipt of SCA legal process. In October 2017, Deputy Attorney General Rod Rosenstein issued a memorandum to DOJ attorneys and agents setting out guidance to ensure that applications for such protective orders are tailored to the specific facts and concerns of an investigation and establishing a general one-year ceiling on how long an application may seek to delay notice. In May 2022, Deputy Attorney General Lisa Monaco issued supplementary guidance on the topic, which among other matters established internal DOJ approval requirements for applications to extend a protective order beyond the initial one-year period and required the termination of protective orders at the close of an investigation.

demonstrate to the judge based on a showing of probable cause that a crime was committed or is about to be committed and that items connected to the crime are likely to be found in the place specified by the warrant. This authority is often used when a physical search by police of a premise is needed due to the danger that evidence may be destroyed if a subpoena or other production order is served on the corporation. A person subject to a search or whose property is subject to a search may move to suppress evidence obtained or derived from an unlawful search if that evidence is introduced against that person during a criminal trial. See *Mapp v. Ohio*, 367 U.S. 643 (1961). When a data holder is required to disclose data pursuant to a warrant, the compelled party may challenge the requirement to disclose as unduly burdensome. See *In re Application of United States*, 610 F.2d 1148, 1157 (3d Cir. 1979) (holding that “due process requires a hearing on the issue of burdensomeness before compelling a telephone company to provide” assistance with a search warrant); *In re Application of United States*, 616 F.2d 1122 (9th Cir. 1980) (reaching same conclusion based on court’s supervisory authority).

DOJ Guidelines and Policies: In addition to these Constitutional, statutory, and rule-based limitations on government access to data, the Attorney General has issued guidelines that place further limits on law enforcement access to data, and that also contain privacy and civil liberties protections. For instance, the Attorney General’s Guidelines for Domestic FBI Operations (September 2008) (hereinafter AG FBI Guidelines), available at <http://www.justice.gov/archive/opa/docs/guidelines.pdf>, set limits on use of investigative means to seek information related to investigations that involve federal crimes. These guidelines require that the FBI use the least intrusive investigative methods feasible, taking into account the effect on privacy and civil liberties and the potential damage to reputation. Further, they note that “it is axiomatic that the FBI must conduct its investigations and other activities in a lawful and reasonable manner that respects liberty and privacy and avoids unnecessary intrusions into the lives of law-abiding people.” AG FBI Guidelines at 5. The FBI has implemented these guidelines through the FBI Domestic Investigations and Operations Guide (DIOG), available at <https://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29>, a comprehensive manual that includes detailed limits on use of investigative tools and guidance to assure that civil liberties and privacy are protected in every investigation. Additional rules and policies that prescribe limitations on the investigative activities of federal prosecutors are set out in the Justice Manual, also available online at <https://www.justice.gov/jm/justice-manual>.

Civil and Regulatory Authorities (Public Interest):

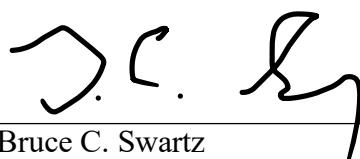
There are also significant limits on civil or regulatory (i.e., “public interest”) access to data held by corporations in the United States. Agencies with civil and regulatory responsibilities may issue subpoenas to corporations for business records, electronically stored information, or other tangible items. These agencies are limited in their exercise of administrative or civil subpoena authority not only by their organic statutes, but also by independent judicial review of subpoenas prior to potential judicial enforcement. See, e.g., Fed. R. Civ. P. 45. Agencies may seek access only to data that is relevant to matters within their scope of authority to regulate. Further, a recipient of an administrative subpoena may challenge the enforcement of that subpoena in court by presenting evidence that the agency has not acted in accordance with basic standards of reasonableness, as discussed earlier.

There are other legal bases for companies to challenge data requests from administrative agencies based on their specific industries and the types of data they possess. For example, financial institutions can challenge administrative subpoenas seeking certain types of information as violations of the Bank Secrecy Act and its implementing regulations. 31 U.S.C. § 5318; 31 C.F.R. Chapter X. Other businesses can rely on the Fair Credit Reporting Act, 15 U.S.C. § 1681b, or a host of other sector specific laws. Misuse of an agency's subpoena authority can result in agency liability, or personal liability for agency officers. See, e.g., Right to Financial Privacy Act, 12 U.S.C. §§ 3401-3423. Courts in the United States thus stand as the guardians against improper regulatory requests and provide independent oversight of federal agency actions.

Finally, any statutory power that administrative authorities have to physically seize records from a company in the United States pursuant to an administrative search must meet requirements based on the Fourth Amendment. See *See v. City of Seattle*, 387 U.S. 541 (1967).

Conclusion:

All law enforcement and regulatory activities in the United States must conform to applicable law, including the U.S. Constitution, statutes, rules, and regulations. Such activities must also comply with applicable policies, including any Attorney General Guidelines governing federal law enforcement activities. The legal framework described above limits the ability of U.S. law enforcement and regulatory agencies to acquire information from corporations in the United States—whether the information concerns U.S. persons or citizens of foreign countries—and in addition permits judicial review of any government requests for data pursuant to these authorities.



Bruce C. Swartz
Deputy Assistant Attorney General and
Counselor for International Affairs

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
OFFICE OF GENERAL COUNSEL
WASHINGTON, DC 20511

December 9, 2022

Leslie B. Kiernan
General Counsel
U.S. Department of Commerce
1401 Constitution Ave., NW
Washington, DC 20230

Dear Ms. Kiernan,

On October 7, 2022, President Biden signed Executive Order 14086, *Enhancing Safeguards for United States Signals Intelligence Activities*, which bolsters the rigorous array of privacy and civil liberties safeguards that apply to U.S. signals intelligence activities. These safeguards include: requiring signals intelligence activities to meet enumerated legitimate objectives; explicitly barring such activities for the purpose of specific prohibited objectives; putting in place novel procedures for ensuring that signals intelligence activities further these legitimate objectives and do not further prohibited objectives; requiring that signals intelligence activities be conducted only following a determination, based on a reasonable assessment of all relevant factors, that the activities are necessary to advance a validated intelligence priority and only to the extent and in a manner that is proportionate to the validated intelligence priority for which they have been authorized; and directing Intelligence Community (IC) elements to update their policies and procedures to reflect the Executive Order's required signals intelligence safeguards. Most significantly, the Executive Order also introduces an independent and binding mechanism enabling individuals from "qualifying states," as designated pursuant to the Executive Order, to seek redress if they believe they were subjected to unlawful U.S. signals intelligence activities, including activities violating the protections found in the Executive Order.

President Biden's issuance of Executive Order 14086 marked the culmination of well over a year of detailed negotiations between representatives from the European Commission (EC) and the United States and directs the steps the United States will take to implement its commitments under the EU-U.S. Data Privacy Framework. Consistent with the cooperative spirit that produced the Framework, it is my understanding that you have received two sets of questions from the EC about how the IC will implement the Executive Order. I am happy to address these questions with this letter.

Section 702 of the Foreign Intelligence Surveillance Act of 1978 (FISA Section 702)

The first set of questions concerns FISA Section 702, which allows the collection of foreign intelligence information through the targeting of non-U.S. persons reasonably believed to be located outside the United States with the compelled assistance of electronic communication service providers. Specifically, the questions concern the interplay between that provision and Executive Order 14086, as well as the other safeguards that apply to activities conducted pursuant to FISA Section 702.

To begin, we can confirm that the IC will apply the safeguards set forth in Executive Order 14086 to activities conducted pursuant to FISA Section 702.

In addition, numerous other safeguards apply to the Government's use of FISA Section 702. For example, all FISA Section 702 certifications must be signed by both the Attorney General and Director of National Intelligence (DNI), and the Government must submit all such certifications for approval by the Foreign Intelligence Surveillance Court (FISC), which is comprised of independent, life-tenured judges who serve non-renewable seven-year terms. The certifications identify categories of foreign intelligence information to be collected, which must meet the statutory definition of foreign intelligence information, through the targeting of non-U.S. persons reasonably believed to be located outside the United States. The certifications have included information concerning international terrorism and other topics, such as the acquisition of information concerning weapons of mass destruction. Each annual certification must be submitted to the FISC for approval in a certification application package that includes the Attorney General's and DNI's certifications, affidavits by certain heads of intelligence agencies, and targeting procedures, minimization procedures, and querying procedures that are binding on the Government. The targeting procedures require, among other things, that the IC reasonably assess, based on the totality of the circumstances, that the targeting will likely lead to the collection of foreign intelligence information identified in a FISA Section 702 certification.

Moreover, when collecting information pursuant to FISA Section 702, the IC must: provide a written explanation of the basis for their assessment, at the time of targeting, that the target is expected to possess, is expected to receive, or is likely to communicate foreign intelligence information identified in a FISA Section 702 certification; confirm that the targeting standard as set forth in FISA Section 702 targeting procedures remains satisfied; and cease collection if the standard is no longer satisfied. *See* U.S. Government Submission to Foreign Intelligence Surveillance Court, *2015 Summary of Notable Section 702 Requirements*, at 2-3 (July 15, 2015).

Requiring the IC to record in writing, and regularly affirm the validity of, its assessment that FISA Section 702 targets meet the applicable targeting standards facilitates the FISC's supervision of the IC's targeting activities. Each recorded targeting assessment and rationale is reviewed on a bimonthly basis by intelligence oversight attorneys in the Department of Justice (DOJ), who conduct this oversight function independently from foreign intelligence operations. The DOJ section performing this function is then responsible under a long-established FISC rule to report to the FISC any violations of the applicable procedures. This reporting, along with regular meetings between the FISC and this DOJ section regarding oversight of FISA Section 702 targeting, enables the FISC to enforce compliance with the FISA Section 702 targeting and other procedures and otherwise ensure that the Government's activities are lawful. In particular, the FISC can do this in a number of ways, including by issuing binding remedial decisions to terminate the Government's authority to collect against a particular target, or to modify or delay FISA Section 702 data collection. The FISC also can require the Government to provide further reporting or briefing on its compliance with targeting and other procedures or require changes to those procedures.

The “Bulk” Collection of Signals Intelligence

The second set of questions concerns the “bulk” collection of signals intelligence, which is defined by Executive Order 14086 as “the authorized collection of large quantities of signals intelligence data that, due to technical or operational considerations, is acquired without the use of discriminants (for example, without the use of specific identifiers or selection terms).”

With respect to these questions, we first note that neither FISA nor National Security Letters authorize bulk collection. With respect to FISA:

- Titles I and III of FISA, which respectively authorize electronic surveillance and physical searches, require a court order (with limited exceptions, such as emergency circumstances) and always require probable cause to believe that the target is a foreign power or an agent of a foreign power. *See* 50 U.S.C. §§ 1805, 1824.
- The USA FREEDOM Act of 2015 amended Title IV of FISA, which authorizes the use of pen registers and trap and trace devices, pursuant to court order (except in emergency circumstances), to require the Government to base requests on a “specific selection term.” *See* 50 U.S.C. § 1842(c)(3).
- Title V of FISA, which permits the Federal Bureau of Investigation (FBI) to obtain certain types of business records, requires a court order based on an application that specifies that “there are specific and articulable facts giving reason to believe that the person to whom the records pertain is a foreign power or an agent of a foreign power.” *See* 50 U.S.C. § 1862(b)(2)(B).¹
- Finally, FISA Section 702 authorizes the “targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information.” *See* 50 U.S.C. § 1881a(a). Thus, as the Privacy and Civil Liberties Oversight Board has noted, the Government’s collection of data under FISA Section 702 “consists entirely of targeting individual persons and acquiring communications associated with those persons, from whom the government has reason to expect it will obtain certain types of foreign intelligence,” such that the “program does not operate by collecting communications in bulk.” Privacy and Civil Liberties Oversight Board, *Report on the*

¹ From 2001 until 2020, Title V of FISA permitted the FBI to seek authorization from the FISC to obtain “tangible things” that are relevant to certain authorized investigations. *See* USA PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272, § 215 (2001). This language, which has sunset and is thus no longer the law, provided the authority pursuant to which the Government at one time collected telephony metadata in bulk. Even before the provision sunset, however, the USA FREEDOM Act had amended it to require the Government to base an application to the FISC on a “specific selection term.” *See* USA FREEDOM Act, Pub. L. No. 114-23, 129 Stat. 268, § 103 (2015).

*Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, at 103 (July 2, 2014).*²

With respect to National Security Letters, the USA FREEDOM Act of 2015 imposes a “specific selection term” requirement on the use of such letters. *See* 12 U.S.C. § 3414(a)(2); 15 U.S.C. § 1681u; 15 U.S.C. § 1681v(a); 18 U.S.C. § 2709(b).

Further, Executive Order 14086 provides that “[t]argeted collection shall be prioritized” and that, when the IC does conduct bulk collection, the “bulk collection of signals intelligence shall be authorized only based on a determination . . . that the information necessary to advance a validated intelligence priority cannot reasonably be obtained by targeted collection.” *See* Executive Order 14086, § 2(c)(ii)(A).

Moreover, when the IC determines that bulk collection satisfies these standards, Executive Order 14086 provides additional safeguards. Specifically, the Executive Order requires the IC, when conducting bulk collection, to “apply reasonable methods and technical measures in order to limit the data collected to only what is necessary to advance a validated intelligence priority, while minimizing the collection of non-pertinent information.” *See id.* The Order also states that “signals intelligence activities,” which include the querying of signals intelligence obtained by bulk collection, “shall be conducted only following a determination, based on a reasonable assessment of all relevant factors, that the activities are necessary to advance a validated intelligence priority.” *See id.* § 2(a)(ii)(A). The Order further implements this principle by stating that the IC may only query unminimized signals intelligence obtained in bulk in pursuit of six permissible objectives, and that such queries must be conducted according to policies and procedures that “appropriately take into account the impact [of the queries] on the privacy and civil liberties of all persons, regardless of their nationality or wherever they might reside.” *See id.* § 2(c)(iii)(D). Lastly, the Order provides for handling, security, and access controls for data collected. *See id.* § 2(c)(iii)(A) and § 2(c)(iii)(B).

* * * * *

We hope these clarifications are of assistance. Please do not hesitate to contact us if you have further questions about how the U.S. IC plans to implement Executive Order 14086.

Sincerely,



Christopher C. Fonzone
General Counsel

² Sections 703 and 704, which authorize the IC to target U.S. persons located overseas, require a court order (except in emergency circumstances) and always require probable cause to believe that the target is a foreign power, an agent of a foreign power, or an officer or employee of a foreign power. *See* 50 U.S.C. §§ 1881b, 1881c.