**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 them[3]. 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 re-certification 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 14086[4] 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 identifiable[7] 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 Principles[8], 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 Principles[9], 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 Principles[15] 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 respond[17]. 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 Principles[18] 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.