NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document : Secure Controls Framework (SCF) version 2025.1
STRM Guidance: https://securecontrolsframework.com/set-theory-relationship-mapping-strm/

Focal Document: **US Data Privacy Framework**
Focal Document URL: https://www.dataprivacyframework.gov/Program-Overview
Published STRM URL: https://securecontrolsframework.com/content/strm/scf-strm-us-fed-data-privacy-framework.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
I	Overview	See law for full details	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
II	Principles	No content	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
II.1	Notice	No content	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
II.1.a	Notice	An organization must inform individuals about:	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
II.1.a.i	Notice	its participation in the EU-U.S. DPF and provide a link to, or the web address for, the Data Privacy Framework List,	Functional	intersects with	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations. (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	5	
II.1.a.ii	Notice	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,	Functional	intersects with	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations. (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	5	
II.1.a.iii	Notice	its commitment to subject to the Principles all personal data received from the EU in reliance on the EU-U.S. DPF,	Functional	intersects with	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations. (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	5	
II.1.a.iv	Notice	the purposes for which it collects and uses personal information about them,	Functional	intersects with	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations. (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	5	
II.1.a.iv	Notice	the purposes for which it collects and uses personal information about them,	Functional	subset of	Purpose Specification	PRI-02.1	Mechanisms exist to ensure the data privacy notice identifies the purpose(s) for which Personal Data (PD) is collected, received, processed, stored, transmitted, shared.	10	
II.1.a.v	Notice	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,	Functional	intersects with	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations. (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	5	
II.1.a.vi	Notice	the type or identity of third parties to which it discloses personal information, and the purposes for which it does so,	Functional	intersects with	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations. (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
II.1.a.vii	Notice	the right of individuals to access their personal data,	Functional	intersects with	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations. (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	5	
II.1.a.viii	Notice	the choices and means the organization offers individuals for limiting the use and disclosure of their personal data,	Functional	intersects with	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations. (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	5	
II.1.a.ix	Notice	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,	Functional	intersects with	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations. (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	5	
II.1.a.x	Notice	being subject to the investigatory and enforcement powers of the FTC, the DOT or any other U.S. authorized statutory body,	Functional	intersects with	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations. (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	5	
II.1.a.xi	Notice	the possibility, under certain conditions, for the individual to invoke binding arbitration,5	Functional	intersects with	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations. (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	5	
II.1.a.xii	Notice	the requirement to disclose personal information in response to lawful requests by public authorities, including to meet national security or law enforcement requirements, and	Functional	intersects with	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations. (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	5	
II.1.a.xiii	Notice	its liability in cases of onward transfers to third parties.	Functional	intersects with	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations. (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
II.1.b	Notice	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.	Functional	intersects with	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations. (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	5	
II.2	Choice	No content	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
II.2.a	Choice	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.	Functional	subset of	Choice & Consent	PRI-03	Mechanisms exist to enable data subjects to authorize the collection, processing, storage, sharing, updating and disposal of their Personal Data (PD), where prior to collection the data subject is provided with: (1) Plain language to illustrate the potential data privacy risks of the authorization; (2) A means for users to decline the authorization; and (3) All necessary choice and consent-related criteria required by applicable statutory, regulatory and contractual obligations.	10	
II.2.b	Choice	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.	Functional	intersects with	Authorized Agent	PRI-03.6	Mechanisms exist to allow data subjects to authorize another person or entity, acting on the data subject's behalf, to make Personal Data (PD) processing decisions.	5	
II.2.c	Choice	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.	Functional	intersects with	Choice & Consent	PRI-03	Mechanisms exist to enable data subjects to authorize the collection, processing, storage, sharing, updating and disposal of their Personal Data (PD), where prior to collection the data subject is provided with: (1) Plain language to illustrate the potential data privacy risks of the authorization; (2) A means for users to decline the authorization; and (3) All necessary choice and consent-related criteria required by applicable statutory, regulatory and contractual obligations.	5	
II.2.c	Choice	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.	Functional	intersects with	Active Participation By Data Subjects	PRI-03.7	Mechanisms exist to compel data subjects to select the level of consent deemed appropriate by the data subject for the relevant business purpose (e.g., opt-in, opt-out, accept all cookies, etc.).	5	
II.2.c	Choice	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.	Functional	intersects with	Usage Restrictions of Personal Data (PD)	PRI-05.4	Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, updating and/or sharing Personal Data (PD) to: (1) The purpose(s) originally collected, consistent with the data privacy notice(s); (2) What is authorized by the data subject, or authorized agent; and (3) What is consistent with applicable laws, regulations and contractual obligations.	5	
II.3	Accountability for Onward Transfer	No content	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
II.3.a	Accountability for Onward Transfer	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.	Functional	subset of	Binding Corporate Rules (BCR)	PRI-01.5	Mechanisms exist to implement and manage Binding Corporate Rules (BCR) (e.g., data sharing agreement) to legally-bind all parties engaged in a joint economic activity that contractually states enforceable rights on data subjects with regard to the processing of their personal data.	10	
II.3.a	Accountability for Onward Transfer	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.	Functional	intersects with	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	5	
II.3.b	Accountability for Onward Transfer	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.	Functional	subset of	Binding Corporate Rules (BCR)	PRI-01.5	Mechanisms exist to implement and manage Binding Corporate Rules (BCR) (e.g., data sharing agreement) to legally-bind all parties engaged in a joint economic activity that contractually states enforceable rights on data subjects with regard to the processing of their personal data.	10	
II.3.b	Accountability for Onward Transfer	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.	Functional	intersects with	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
II.4	Security	No content	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
II.4.a	Security	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.	Functional	subset of	Operationalizing Cybersecurity & Data Protection Practices	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize cybersecurity & data privacy practices for each system, application and/or service under their control.	10	
II.4.a	Security	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.	Functional	subset of	Security of Personal Data (PD)	PRI-01.6	Mechanisms exist to ensure Personal Data (PD) is protected by logical and physical security safeguards that are sufficient and appropriately scoped to protect the confidentiality and integrity of the PD.	10	
II.4.a	Security	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.	Functional	subset of	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized cybersecurity & data privacy practices in the specification, design, development, implementation and modification of systems and services.	10	
II.5	Data Integrity and Purpose Limitation	No content	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
II.5.a	Data Integrity and Purpose Limitation	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 current. An organization must adhere to the Principles for as long as it retains such information.	Functional	intersects with	Purpose Specification	PRI-02.1	Mechanisms exist to ensure the data privacy notice identifies the purpose(s) for which Personal Data (PD) is collected, received, processed, stored, transmitted, shared.	5	
II.5.a	Data Integrity and Purpose Limitation	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 current. An organization must adhere to the Principles for as long as it retains such information.	Functional	intersects with	Restrict Collection To Identified Purpose	PRI-04	Mechanisms exist to minimize the collection of Personal Data (PD) to only what is adequate, relevant and limited to the purposes identified in the data privacy notice, including protections against collecting PD from minors without appropriate parental or legal guardian consent.	5	
II.5.a	Data Integrity and Purpose Limitation	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 current. An organization must adhere to the Principles for as long as it retains such information.	Functional	intersects with	Validate Collected Personal Data (PD)	PRI-04.5	Mechanisms exist to ensure that the data subject, or authorized representative, validate Personal Data (PD) during the collection process.	5	
II.5.a	Data Integrity and Purpose Limitation	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 current. An organization must adhere to the Principles for as long as it retains such information.	Functional	intersects with	Personal Data (PD) Accuracy & Integrity	PRI-05.2	Mechanisms exist to ensure the accuracy and relevance of Personal Data (PD) throughout the information lifecycle by: (1) Keeping PD up-to-date; and (2) Remediating identified inaccuracies, as necessary.	5	
II.5.b	Data Integrity and Purpose Limitation	Information may be retained in a form identifying or making identifiable7 the individual only for as long as it serves a purpose of processing within the meaning of 5(a). This obligation does not prevent organizations from processing personal information for longer periods for the time and to the extent such processing reasonably serves the purposes of archiving in the public interest, journalism, literature and art, scientific or historical research, and statistical analysis. In these cases, such processing shall be subject to the other principles and provisions of the EU-U.S. DPF. Organizations should take reasonable and appropriate measures in complying with this provision.	Functional	intersects with	Personal Data (PD) Retention & Disposal	PRI-05	Mechanisms exist to: (1) Retain Personal Data (PD), including metadata, for an organization-defined time period to fulfill the purpose(s) identified in the notice or as required by law; (2) Dispose of, destroys, erases, and/or anonymizes the PD, regardless of the method of storage; and (3) Use organization-defined techniques or methods to ensure secure deletion or destruction of PD (including originals, copies and archived records).	5	
II.6	Access	No content	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
II.6.a	Access	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.	Functional	subset of	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to: (1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the benefit offered to the data subject through granting access; (2) Obtain answers on the specifics of how their PD is collected, received, processed, stored, transmitted, shared, updated and disposed; (3) Obtain the source(s) of their PD; (4) Obtain the categories of their PD being collected, received, processed, stored and shared; (5) Request correction to their PD due to inaccuracies; (6) Request erasure of their PD; and (7) Restrict the further collecting, receiving, processing, storing, transmitting, updated and/or sharing of their PD.	10	
II.6.a	Access	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.	Functional	intersects with	Correcting Inaccurate Personal Data	PRI-06.1	Mechanisms exist to establish and implement a process for: (1) Data subjects to have inaccurate Personal Data (PD) maintained by the organization corrected or amended; and (2) Disseminating corrections or amendments of PD to other authorized users of the PD.	5	
II.7	Recourse, Enforcement and Liability	No content	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
II.7.a	Recourse, Enforcement and Liability	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:	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
II.7.a.i	Recourse, Enforcement and Liability	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;	Functional	intersects with	User Feedback Management	PRI-06.4	Mechanisms exist to maintain a process to efficiently and effectively respond to complaints, concerns or questions from authenticated data subjects about how the organization collects, receives, processes, stores, transmits, shares, updates and/or disposes of their Personal Data (PD).	5	
II.7.a.ii	Recourse, Enforcement and Liability	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 noncompliance; and	Functional	intersects with	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	5	
II.7.a.iii	Recourse, Enforcement and Liability	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 must be sufficiently rigorous to ensure compliance by organizations.	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
II.7.b	Recourse, Enforcement and Liability	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.	Functional	intersects with	Ability To Demonstrate Conformity	CPL-01.3	Mechanisms exist to ensure the organization is able to demonstrate conformity with applicable cybersecurity and data protection laws, regulations and/or contractual obligations.	5	
II.7.c	Recourse, Enforcement and Liability	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.	Functional	subset of	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	10	
II.7.d	Recourse, Enforcement and Liability	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.	Functional	intersects with	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	5	
II.7.d	Recourse, Enforcement and Liability	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.	Functional	intersects with	Contract Flow-Down Requirements	TPM-05.2	Mechanisms exist to ensure cybersecurity & data privacy requirements are included in contracts that flow-down to applicable sub-contractors and suppliers.	5	
II.7.e	Recourse, Enforcement and Liability	When an organization becomes subject to a court order that is based on noncompliance 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.	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III	Supplemental Principles	No content	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.1	Sensitive Data	No content	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.1.a	Sensitive Data	An organization is not required to obtain affirmative, express consent (i.e., opt in) with respect to sensitive data where the processing is:	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.1.a.i	Sensitive Data	in the vital interests of the data subject or another person;	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.1.a.ii	Sensitive Data	necessary for the establishment of legal claims or defenses;	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.1.a.iii	Sensitive Data	required to provide medical care or diagnosis;	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.1.a.iv	Sensitive Data	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;	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.1.a.v	Sensitive Data	necessary to carry out the organization's obligations in the field of employment law; or	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.1.a.vi	Sensitive Data	related to data that are manifestly made public by the individual.	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.2	Journalistic Exceptions	No content	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.2.a	Journalistic Exceptions	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.	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.2.b	Journalistic Exceptions	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.	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.3	Secondary Liability	No content	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.3.a	Secondary Liability	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.	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.4	Performing Due Diligence and Conducting Audits	No content	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.4.a	Performing Due Diligence and Conducting Audits	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.	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.4.b	Performing Due Diligence and Conducting Audits	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.	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.5	The Role of the Data Protection Authorities	No content	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
III.5.a	The Role of the Data Protection Authorities	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.	Functional	subset of	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	10	
III.5.a	The Role of the Data Protection Authorities	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.	Functional	intersects with	Ability To Demonstrate Conformity	CPL-01.3	Mechanisms exist to ensure the organization is able to demonstrate conformity with applicable cybersecurity and data protection laws, regulations and/or contractual obligations.	5	
III.5.b	The Role of the Data Protection Authorities	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:	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.5.b.i	The Role of the Data Protection Authorities	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;	Functional	subset of	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	10	
III.5.b.ii	The Role of the Data Protection Authorities	will cooperate with the DPAs in the investigation and resolution of complaints brought under the Principles; and	Functional	intersects with	Investigation Access Restrictions	CPL-05.2	Mechanisms exist to support official investigations by provisioning government investigators with "least privileges" and "least functionality" to ensure that government investigators only have access to the data and systems needed to perform the investigation.	5	
III.5.b.iii	The Role of the Data Protection Authorities	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.	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.5.c	The Role of the Data Protection Authorities	Operation of DPA Panels	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.5.c.i	The Role of the Data Protection Authorities	The cooperation of the DPAs will be provided in the form of information and advice in the following way:	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.5.c.i.1	The Role of the Data Protection Authorities	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.	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.5.c.i.2	The Role of the Data Protection Authorities	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.	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.5.c.i.3	The Role of the Data Protection Authorities	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.	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.5.c.i.4	The Role of the Data Protection Authorities	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.	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.5.c.i.5	The Role of the Data Protection Authorities	The panel will make public the results of its consideration of complaints submitted to it, if it sees fit.	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.5.c.i.6	The Role of the Data Protection Authorities	The delivery of advice through the panel will not give rise to any liability for the panel or for individual DPAs.	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.5.c.ii	The Role of the Data Protection Authorities	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.	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.5.d	The Role of the Data Protection Authorities	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).	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.5.e	The Role of the Data Protection Authorities	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.	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.6	Self-Certification	No content	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
III.6.a	Self-Certification	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).	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.6.b	Self-Certification	To initially self-certify or subsequently re-certify for the EU-U.S. DPF, an organization must on each occasion provide to the Department a submission by a corporate officer on behalf of the organization that is self-certifying or re-certifying (as applicable) its adherence to the Principles8, that contains at least the following information:	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.6.b.i	Self-Certification	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;	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.6.b.ii	Self-Certification	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;	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.6.b.iii	Self-Certification	a description of the organization's relevant privacy policy/ies for such personal information, including:	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.6.b.iii.1	Self-Certification	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	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.6.b.iii.2	Self-Certification	its effective date of implementation;	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.6.b.iv	Self-Certification	a contact office within the organization for the handling of complaints, access requests, and any other issues arising under the Principles9, including:	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.6.b.iv.1	Self-Certification	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	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.6.b.iv.2	Self-Certification	the relevant U.S. mailing address for the organization;	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.6.b.v	Self-Certification	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);	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.6.b.vi	Self-Certification	the name of any privacy program in which the organization is a member;	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.6.b.vii	Self-Certification	the method of verification (i.e., self-assessment; or outside compliance reviews, including the third party that completes such reviews);10 and	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.6.b.viii	Self-Certification	the relevant independent recourse mechanism(s) available to investigate unresolved Principles-related complaints.11	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.6.c	Self-Certification	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.	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.6.d	Self-Certification	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.	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.6.e	Self-Certification	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.	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.6.f	Self-Certification	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.	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
III.6.g	Self-Certification	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 selfcertification 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.	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.6.h	Self-Certification	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 EUU. S. DPF. The EU-U.S. DPF certification mark, if used, must also be 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).	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.7	Verification	No content	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.7.a	Verification	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.	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.7.b	Verification	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.	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.7.c	Verification	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.	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.7.d	Verification	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.	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.7.e	Verification	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.	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.8	Access	No content	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.8.a	Access	The Access Principle in Practice	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.8.a.i	Access	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:	Functional	intersects with	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to: (1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the benefit offered to the data subject through granting access; (2) Obtain answers on the specifics of how their PD is collected, received, processed, stored, transmitted, shared, updated and disposed; (3) Obtain the source(s) of their PD; (4) Obtain the categories of their PD being collected, received, processed, stored and shared; (5) Request correction to their PD due to inaccuracies; (6) Request erasure of their PD; and (7) Restrict the further collecting, receiving, processing, storing, transmitting, updated and/or sharing of their PD.	5	
III.8.a.i.1	Access	obtain from an organization confirmation of whether or not the organization is processing personal data relating to them;14	Functional	intersects with	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to: (1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the benefit offered to the data subject through granting access; (2) Obtain answers on the specifics of how their PD is collected, received, processed, stored, transmitted, shared, updated and disposed; (3) Obtain the source(s) of their PD; (4) Obtain the categories of their PD being collected, received, processed, stored and shared; (5) Request correction to their PD due to inaccuracies; (6) Request erasure of their PD; and (7) Restrict the further collecting, receiving, processing, storing, transmitting, updated and/or sharing of their PD.	5	
III.8.a.i.2	Access	have communicated to them such data so that they could verify its accuracy and the lawfulness of the processing; and	Functional	intersects with	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to: (1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the benefit offered to the data subject through granting access; (2) Obtain answers on the specifics of how their PD is collected, received, processed, stored, transmitted, shared, updated and disposed; (3) Obtain the source(s) of their PD; (4) Obtain the categories of their PD being collected, received, processed, stored and shared; (5) Request correction to their PD due to inaccuracies; (6) Request erasure of their PD; and (7) Restrict the further collecting, receiving, processing, storing, transmitting, updated and/or sharing of their PD.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
III.8.a.i.3	Access	have the data corrected, amended or deleted where it is inaccurate or processed in violation of the Principles.	Functional	intersects with	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to: (1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the benefit offered to the data subject through granting access; (2) Obtain answers on the specifics of how their PD is collected, received, processed, stored, transmitted, shared, updated and disposed; (3) Obtain the source(s) of their PD; (4) Obtain the categories of their PD being collected, received, processed, stored and shared; (5) Request correction to their PD due to inaccuracies; (6) Request erasure of their PD; and (7) Restrict the further collecting, receiving, processing, storing, transmitting, updated and/or sharing of their PD.	5	
III.8.a.iii	Access	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.	Functional	intersects with	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to: (1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the benefit offered to the data subject through granting access; (2) Obtain answers on the specifics of how their PD is collected, received, processed, stored, transmitted, shared, updated and disposed; (3) Obtain the source(s) of their PD; (4) Obtain the categories of their PD being collected, received, processed, stored and shared; (5) Request correction to their PD due to inaccuracies; (6) Request erasure of their PD; and (7) Restrict the further collecting, receiving, processing, storing, transmitting, updated and/or sharing of their PD.	5	
III.8.b	Access	Burden or Expense of Providing Access	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.8.b.i	Access	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.	Functional	intersects with	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to: (1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the benefit offered to the data subject through granting access; (2) Obtain answers on the specifics of how their PD is collected, received, processed, stored, transmitted, shared, updated and disposed; (3) Obtain the source(s) of their PD; (4) Obtain the categories of their PD being collected, received, processed, stored and shared; (5) Request correction to their PD due to inaccuracies; (6) Request erasure of their PD; and (7) Restrict the further collecting, receiving, processing, storing, transmitting, updated and/or sharing of their PD.	5	
III.8.b.ii	Access	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.	Functional	intersects with	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to: (1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the benefit offered to the data subject through granting access; (2) Obtain answers on the specifics of how their PD is collected, received, processed, stored, transmitted, shared, updated and disposed; (3) Obtain the source(s) of their PD; (4) Obtain the categories of their PD being collected, received, processed, stored and shared; (5) Request correction to their PD due to inaccuracies; (6) Request erasure of their PD; and (7) Restrict the further collecting, receiving, processing, storing, transmitting, updated and/or sharing of their PD.	5	
III.8.c	Access	Confidential Commercial Information	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.8.c.i	Access	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.	Functional	intersects with	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive / regulated data to authorized parties with a need to know.	5	
III.8.c.ii	Access	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 nonconfidential information.	Functional	intersects with	Limiting Personal Data (PD) Disclosures	PRI-01.7	Mechanisms exist to limit the disclosure of Personal Data (PD) to authorized parties for the sole purpose for which the PD was obtained.	5	
III.8.d	Access	Organization of Data Bases	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.8.d.i	Access	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.	Functional	intersects with	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive / regulated data to authorized parties with a need to know.	5	
III.8.d.ii	Access	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.	Functional	intersects with	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to: (1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the benefit offered to the data subject through granting access; (2) Obtain answers on the specifics of how their PD is collected, received, processed, stored, transmitted, shared, updated and disposed; (3) Obtain the source(s) of their PD; (4) Obtain the categories of their PD being collected, received, processed, stored and shared; (5) Request correction to their PD due to inaccuracies; (6) Request erasure of their PD; and (7) Restrict the further collecting, receiving, processing, storing, transmitting, updated and/or sharing of their PD.	5	
III.8.d.ii	Access	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.	Functional	intersects with	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to: (1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the benefit offered to the data subject through granting access; (2) Obtain answers on the specifics of how their PD is collected, received, processed, stored, transmitted, shared, updated and disposed; (3) Obtain the source(s) of their PD; (4) Obtain the categories of their PD being collected, received, processed, stored and shared; (5) Request correction to their PD due to inaccuracies; (6) Request erasure of their PD; and (7) Restrict the further collecting, receiving, processing, storing, transmitting, updated and/or sharing of their PD.	5	
III.8.e	Access	When Access May be Restricted	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.8.e.i	Access	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:	Functional	intersects with	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to: (1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the benefit offered to the data subject through granting access; (2) Obtain answers on the specifics of how their PD is collected, received, processed, stored, transmitted, shared, updated and disposed; (3) Obtain the source(s) of their PD; (4) Obtain the categories of their PD being collected, received, processed, stored and shared; (5) Request correction to their PD due to inaccuracies; (6) Request erasure of their PD; and (7) Restrict the further collecting, receiving, processing, storing, transmitting, updated and/or sharing of their PD.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
III.8.e.i.1	Access	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;	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.8.e.i.2	Access	disclosure where the legitimate rights or important interests of others would be violated;	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.8.e.i.3	Access	breaching a legal or other professional privilege or obligation;	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.8.e.i.4	Access	prejudicing employee security investigations or grievance proceedings or in connection with employee succession planning and corporate re-organizations; or	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.8.e.i.5	Access	prejudicing the confidentiality necessary in monitoring, inspection or regulatory functions connected with sound management, or in future or ongoing negotiations involving the organization.	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.8.e.ii	Access	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.	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.8.f	Access	Right to Obtain Confirmation and Charging a Fee to Cover the Costs for Providing Access	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.8.f.i	Access	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.	Functional	intersects with	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to: (1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the benefit offered to the data subject through granting access; (2) Obtain answers on the specifics of how their PD is collected, received, processed, stored, transmitted, shared, updated and disposed; (3) Obtain the source(s) of their PD; (4) Obtain the categories of their PD being collected, received, processed, stored and shared; (5) Request correction to their PD due to inaccuracies; (6) Request erasure of their PD; and (7) Restrict the further collecting, receiving, processing, storing, transmitting, updated and/or sharing of their PD.	5	
III.8.f.ii	Access	Charging a fee may be justified, for example, where requests for access are manifestly excessive, in particular because of their repetitive character.	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.8.f.iii	Access	Access may not be refused on cost grounds if the individual offers to pay the costs.	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.8.g	Access	Repetitious or Vexatious Requests for Access	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.8.g.i	Access	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.	Functional	intersects with	Justification To Reject Disclosure Requests	PRI-07.5	Mechanisms exist to reject data subject access requests that are categorized as: (1) Harassing; (2) Repetitive; or (3) Fraudulent.	5	
III.8.h	Access	Fraudulent Requests for Access	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.8.h.i	Access	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.	Functional	intersects with	Justification To Reject Disclosure Requests	PRI-07.5	Mechanisms exist to reject data subject access requests that are categorized as: (1) Harassing; (2) Repetitive; or (3) Fraudulent.	5	
III.8.i	Access	Timeframe for Responses	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.8.i.i	Access	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.	Functional	intersects with	User Feedback Management	PRI-06.4	Mechanisms exist to maintain a process to efficiently and effectively respond to complaints, concerns or questions from authenticated data subjects about how the organization collects, receives, processes, stores, transmits, shares, updates and/or disposes of their Personal Data (PD).	5	
III.9	Human Resources Data	No content	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.9.a	Human Resources Data	Coverage by the EU-U.S. DPF	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.9.a.i	Human Resources Data	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 EUU. 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.	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.9.a.ii	Human Resources Data	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.	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.9.b	Human Resources Data	Application of the Notice and Choice Principles	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.9.b.i	Human Resources Data	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-employmentrelated 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.	Functional	intersects with	Binding Corporate Rules (BCR)	PRI-01.5	Mechanisms exist to implement and manage Binding Corporate Rules (BCR) (e.g., data sharing agreement) to legally-bind all parties engaged in a joint economic activity that contractually states enforceable rights on data subjects with regard to the processing of their personal data.	5	
III.9.b.ii	Human Resources Data	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.	Functional	intersects with	Binding Corporate Rules (BCR)	PRI-01.5	Mechanisms exist to implement and manage Binding Corporate Rules (BCR) (e.g., data sharing agreement) to legally-bind all parties engaged in a joint economic activity that contractually states enforceable rights on data subjects with regard to the processing of their personal data.	5	
III.9.b.iii	Human Resources Data	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.	Functional	subset of	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	10	
III.9.b.iii	Human Resources Data	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.	Functional	intersects with	Binding Corporate Rules (BCR)	PRI-01.5	Mechanisms exist to implement and manage Binding Corporate Rules (BCR) (e.g., data sharing agreement) to legally-bind all parties engaged in a joint economic activity that contractually states enforceable rights on data subjects with regard to the processing of their personal data.	5	
III.9.b.iv	Human Resources Data	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.	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.9.c	Human Resources Data	Application of the Access Principle	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
III.9.c.i	Human Resources Data	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.	Functional	intersects with	Binding Corporate Rules (BCR)	PRI-01.5	Mechanisms exist to implement and manage Binding Corporate Rules (BCR) (e.g., data sharing agreement) to legally-bind all parties engaged in a joint economic activity that contractually states enforceable rights on data subjects with regard to the processing of their personal data.	5	
III.9.d	Human Resources Data	Enforcement	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.9.d.i	Human Resources Data	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.	Functional	intersects with	Binding Corporate Rules (BCR)	PRI-01.5	Mechanisms exist to implement and manage Binding Corporate Rules (BCR) (e.g., data sharing agreement) to legally-bind all parties engaged in a joint economic activity that contractually states enforceable rights on data subjects with regard to the processing of their personal data.	5	
III.9.d.ii	Human Resources Data	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.	Functional	intersects with	Binding Corporate Rules (BCR)	PRI-01.5	Mechanisms exist to implement and manage Binding Corporate Rules (BCR) (e.g., data sharing agreement) to legally-bind all parties engaged in a joint economic activity that contractually states enforceable rights on data subjects with regard to the processing of their personal data.	5	
III.9.e	Human Resources Data	Application of the Accountability for Onward Transfer Principle	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.9.e.i	Human Resources Data	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.	Functional	intersects with	Binding Corporate Rules (BCR)	PRI-01.5	Mechanisms exist to implement and manage Binding Corporate Rules (BCR) (e.g., data sharing agreement) to legally-bind all parties engaged in a joint economic activity that contractually states enforceable rights on data subjects with regard to the processing of their personal data.	5	
III.10	Obligatory Contracts for Onward Transfers	No content	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.10.a	Obligatory Contracts for Onward Transfers	Data Processing Contracts	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.10.a.i	Obligatory Contracts for Onward Transfers	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.	Functional	intersects with	Binding Corporate Rules (BCR)	PRI-01.5	Mechanisms exist to implement and manage Binding Corporate Rules (BCR) (e.g., data sharing agreement) to legally-bind all parties engaged in a joint economic activity that contractually states enforceable rights on data subjects with regard to the processing of their personal data.	5	
III.10.a.i	Obligatory Contracts for Onward Transfers	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.	Functional	intersects with	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	5	
III.10.a.ii	Obligatory Contracts for Onward Transfers	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:	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.10.a.ii.1	Obligatory Contracts for Onward Transfers	acts only on instructions from the controller;	Functional	intersects with	Binding Corporate Rules (BCR)	PRI-01.5	Mechanisms exist to implement and manage Binding Corporate Rules (BCR) (e.g., data sharing agreement) to legally-bind all parties engaged in a joint economic activity that contractually states enforceable rights on data subjects with regard to the processing of their personal data.	5	
III.10.a.ii.1	Obligatory Contracts for Onward Transfers	acts only on instructions from the controller;	Functional	intersects with	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	5	
III.10.a.ii.1	Obligatory Contracts for Onward Transfers	acts only on instructions from the controller;	Functional	intersects with	Contract Flow-Down Requirements	TPM-05.2	Mechanisms exist to ensure cybersecurity & data privacy requirements are included in contracts that flow-down to applicable sub-contractors and suppliers.	5	
III.10.a.ii.2	Obligatory Contracts for Onward Transfers	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	Functional	intersects with	Binding Corporate Rules (BCR)	PRI-01.5	Mechanisms exist to implement and manage Binding Corporate Rules (BCR) (e.g., data sharing agreement) to legally-bind all parties engaged in a joint economic activity that contractually states enforceable rights on data subjects with regard to the processing of their personal data.	5	
III.10.a.ii.2	Obligatory Contracts for Onward Transfers	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	Functional	intersects with	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	5	
III.10.a.ii.2	Obligatory Contracts for Onward Transfers	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	Functional	intersects with	Contract Flow-Down Requirements	TPM-05.2	Mechanisms exist to ensure cybersecurity & data privacy requirements are included in contracts that flow-down to applicable sub-contractors and suppliers.	5	
III.10.a.ii.3	Obligatory Contracts for Onward Transfers	taking into account the nature of the processing, assists the controller in responding to individuals exercising their rights under the Principles.	Functional	intersects with	Binding Corporate Rules (BCR)	PRI-01.5	Mechanisms exist to implement and manage Binding Corporate Rules (BCR) (e.g., data sharing agreement) to legally-bind all parties engaged in a joint economic activity that contractually states enforceable rights on data subjects with regard to the processing of their personal data.	5	
III.10.a.ii.3	Obligatory Contracts for Onward Transfers	taking into account the nature of the processing, assists the controller in responding to individuals exercising their rights under the Principles.	Functional	intersects with	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	5	
III.10.a.ii.3	Obligatory Contracts for Onward Transfers	taking into account the nature of the processing, assists the controller in responding to individuals exercising their rights under the Principles.	Functional	intersects with	Contract Flow-Down Requirements	TPM-05.2	Mechanisms exist to ensure cybersecurity & data privacy requirements are included in contracts that flow-down to applicable sub-contractors and suppliers.	5	
III.10.a.iii	Obligatory Contracts for Onward Transfers	Because adequate protection is provided by participating organizations, contracts with such organizations for mere processing do not require prior authorization.	Functional	intersects with	Binding Corporate Rules (BCR)	PRI-01.5	Mechanisms exist to implement and manage Binding Corporate Rules (BCR) (e.g., data sharing agreement) to legally-bind all parties engaged in a joint economic activity that contractually states enforceable rights on data subjects with regard to the processing of their personal data.	5	
III.10.a.iii	Obligatory Contracts for Onward Transfers	Because adequate protection is provided by participating organizations, contracts with such organizations for mere processing do not require prior authorization.	Functional	intersects with	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	5	
III.10.a.iii	Obligatory Contracts for Onward Transfers	Because adequate protection is provided by participating organizations, contracts with such organizations for mere processing do not require prior authorization.	Functional	intersects with	Contract Flow-Down Requirements	TPM-05.2	Mechanisms exist to ensure cybersecurity & data privacy requirements are included in contracts that flow-down to applicable sub-contractors and suppliers.	5	
III.10.b	Obligatory Contracts for Onward Transfers	Transfers within a Controlled Group of Corporations or Entities	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.10.b.i	Obligatory Contracts for Onward Transfers	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.	Functional	intersects with	Binding Corporate Rules (BCR)	PRI-01.5	Mechanisms exist to implement and manage Binding Corporate Rules (BCR) (e.g., data sharing agreement) to legally-bind all parties engaged in a joint economic activity that contractually states enforceable rights on data subjects with regard to the processing of their personal data.	5	
III.10.c	Obligatory Contracts for Onward Transfers	Transfers between Controllers	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
III.10.c.i	Obligatory Contracts for Onward Transfers	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.	Functional	intersects with	Binding Corporate Rules (BCR)	PRI-01.5	Mechanisms exist to implement and manage Binding Corporate Rules (BCR) (e.g., data sharing agreement) to legally-bind all parties engaged in a joint economic activity that contractually states enforceable rights on data subjects with regard to the processing of their personal data.	5	
III.11	Dispute Resolution and Enforcement	No content	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.11.a	Dispute Resolution and Enforcement	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.	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.11.b	Dispute Resolution and Enforcement	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.	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.11.c	Dispute Resolution and Enforcement	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.	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.11.d	Dispute Resolution and Enforcement	Recourse Mechanisms	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.11.d.i	Dispute Resolution and Enforcement	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.	Functional	intersects with	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations. (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	5	
III.11.d.i	Dispute Resolution and Enforcement	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.	Functional	intersects with	User Feedback Management	PRI-06.4	Mechanisms exist to maintain a process to efficiently and effectively respond to complaints, concerns or questions from authenticated data subjects about how the organization collects, receives, processes, stores, transmits, shares, updates and/or disposes of their Personal Data (PD).	5	
III.11.d.ii	Dispute Resolution and Enforcement	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 EUU. 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.	Functional	intersects with	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations. (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
III.11.d.iii	Dispute Resolution and Enforcement	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.	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.11.d.iv	Dispute Resolution and Enforcement	As set forth in Annex I, an arbitration option is available to an individual to determine, for residual claims, whether a participating organization has violated its obligations under the Principles as to that individual, and whether any such violation remains fully or partially unremedied. This option is available only for these purposes. This option is not available, for example, with respect to the exceptions to the Principles15 or with respect to an allegation about the adequacy of the EU-U.S. DPF. Under this arbitration option, the "EU-U.S. Data Privacy Framework Panel" (consisting of one or three arbitrators, as agreed by the parties) has the authority to impose individualspecific, 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.	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.11.e	Dispute Resolution and Enforcement	Remedies and Sanctions	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.11.e.i	Dispute Resolution and Enforcement	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 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.	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.11.f	Dispute Resolution and Enforcement	FTC Action	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.11.f.i	Dispute Resolution and Enforcement	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.	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.11.g	Dispute Resolution and Enforcement	Persistent Failure to Comply	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.11.g.i	Dispute Resolution and Enforcement	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.	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.11.g.ii	Dispute Resolution and Enforcement	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, 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.	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.11.g.iii	Dispute Resolution and Enforcement	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 noncompliance from the organization itself, a privacy selfregulatory body or another independent dispute resolution body, or a government body, but only after first providing the organization with 30 days' notice and an opportunity to respond17. Accordingly, the Data Privacy Framework List maintained by the Department will make clear which organizations are assured and which organizations are no longer assured of EU-U.S. DPF benefits.	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.11.g.iv	Dispute Resolution and Enforcement	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.	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.12	Choice - Timing of Opt Out	No content	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.12.a	Choice - Timing of Opt Out	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.	Functional	intersects with	Active Participation By Data Subjects	PRI-03.7	Mechanisms exist to compel data subjects to select the level of consent deemed appropriate by the data subject for the relevant business purpose (e.g., opt-in, opt-out, accept all cookies, etc.).	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
III.12.b	Choice - Timing of Opt Out	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 individual) to receive any further direct marketing communications and the organization complies with the individual's wishes.	Functional	intersects with	Active Participation By Data Subjects	PRI-03.7	Mechanisms exist to compel data subjects to select the level of consent deemed appropriate by the data subject for the relevant business purpose (e.g., opt-in, opt-out, accept all cookies, etc.).	5	
III.13	Travel Information	No content	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.13.a	Travel Information	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 EUU. 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.	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.14	Pharmaceutical and Medical Products	No content	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.14.a	Pharmaceutical and Medical Products	Application of EU/Member State Laws or the Principles	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.14.a.i	Pharmaceutical and Medical Products	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.	Functional	intersects with	De-Identification (Anonymization)	DCH-23	Mechanisms exist to anonymize data by removing Personal Data (PD) from datasets.	5	
III.14.b	Pharmaceutical and Medical Products	Future Scientific Research	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.14.b.i	Pharmaceutical and Medical Products	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.	Functional	intersects with	Just-In-Time Notice & Updated Consent	PRI-03.2	Mechanisms exist to present data subjects with a new or updated consent request to process, store and/or share Personal Data (PD) in conjunction with the data action, when: (1) The original circumstances under which an individual gave consent have changed; or (2) A significant amount of time has passed since an individual gave consent.	5	
III.14.b.ii	Pharmaceutical and Medical Products	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.	Functional	intersects with	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations. (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	5	
III.14.b.ii	Pharmaceutical and Medical Products	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.	Functional	intersects with	Just-In-Time Notice & Updated Consent	PRI-03.2	Mechanisms exist to present data subjects with a new or updated consent request to process, store and/or share Personal Data (PD) in conjunction with the data action, when: (1) The original circumstances under which an individual gave consent have changed; or (2) A significant amount of time has passed since an individual gave consent.	5	
III.14.c	Pharmaceutical and Medical Products	Withdrawal from a Clinical Trial	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.14.c.i	Pharmaceutical and Medical Products	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.	Functional	intersects with	Continued Use of Personal Data (PD)	PRI-03.9	Mechanisms exist to govern the continued use of Personal Data (PD) as it is collected, received, processed, stored, transmitted and/or shared until: (1) Disposal of PD occurs when there is no longer a legitimate business purpose; (2) Disposal of PD occurs when the data retention timeline for the use case is met; and/or (3) Continued use of PD is prohibited upon withdrawal of data subject consent.	5	
III.14.d	Pharmaceutical and Medical Products	Transfers for Regulatory and Supervision Purposes	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.14.d.i	Pharmaceutical and Medical Products	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.	Functional	intersects with	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive / regulated data to authorized parties with a need to know.	5	
III.14.e	Pharmaceutical and Medical Products	"Blinded" Studies	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.14.e.i	Pharmaceutical and Medical Products	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.	Functional	intersects with	Limiting Personal Data (PD) Disclosures	PRI-01.7	Mechanisms exist to limit the disclosure of Personal Data (PD) to authorized parties for the sole purpose for which the PD was obtained.	5	
III.14.e.ii	Pharmaceutical and Medical Products	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.	Functional	intersects with	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to: (1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the benefit offered to the data subject through granting access; (2) Obtain answers on the specifics of how their PD is collected, received, processed, stored, transmitted, shared, updated and disposed; (3) Obtain the source(s) of their PD; (4) Obtain the categories of their PD being collected, received, processed, stored and shared; (5) Request correction to their PD due to inaccuracies; (6) Request erasure of their PD; and (7) Restrict the further collecting, receiving, processing, storing, transmitting, updated and/or sharing of their PD.	5	
III.14.f	Pharmaceutical and Medical Products	Product Safety and Efficacy Monitoring	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
III.14.f.i	Pharmaceutical and Medical Products	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.	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.14.g	Pharmaceutical and Medical Products	Key-coded Data	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.14.g.i	Pharmaceutical and Medical Products	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.	Functional	intersects with	De-Identification (Anonymization)	DCH-23	Mechanisms exist to anonymize data by removing Personal Data (PD) from datasets.	5	
III.15	Public Record and Publicly Available Information	No content	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.15.a	Public Record and Publicly Available Information	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).	Functional	subset of	Data Privacy Program	PRI-01	Mechanisms exist to facilitate the implementation and operation of data protection controls throughout the data lifecycle to ensure all forms of Personal Data (PD) are processed lawfully, fairly and transparently.	10	
III.15.b	Public Record and Publicly Available Information	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.	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.15.c	Public Record and Publicly Available Information	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.	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.15.d	Public Record and Publicly Available Information	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.	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.15.e	Public Record and Publicly Available Information	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.	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.16	Access Requests by Public Authorities	No content	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.16.a	Access Requests by Public Authorities	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.	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.16.b	Access Requests by Public Authorities	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.	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
III.16.c	Access Requests by Public Authorities	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.	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	