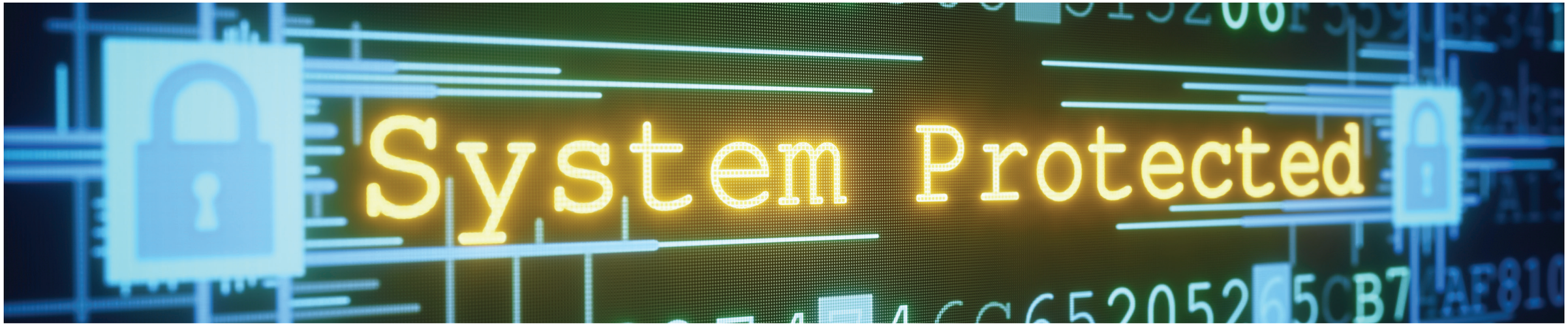
New privacy framework certification vs previous privacy shield certification

2023 EU-U.S. Data Privacy Framework (DPF)	2016 EU-U.S. Data Privacy Shield (DPS)
Principles	
Principles and supplemental principles remain the same.	
DPA Panel fee	
• There will remain an annual fee to cover operating costs of the DPA Panel but the amount will be determined by the U.S. Department of Commerce (DoC) after consultation with the European Commission. • DPA Panel fee, payable to the United States Council for International Business (USCIB), determined to be $50.	• Organizations opting for or being obliged to use the DPA Panel as a dispute resolution mechanism were required to pay an annual fee to cover operating costs of the DPA Panel, not exceeding $500. (See section on redress mechanism below.)
Redress mechanism	
Relating to organization's compliance with privacy principles (the Principles)	
Data subjects have the same core redress mechanisms against an organization and may: • Lodge a complaint with the organization. • Lodge a complaint to the national Data Protection Authority (DPA), which will investigate and resolve, or refer the complaint to the competent U.S. authority. • Invoke binding free of charge dispute resolution mechanism, which can either be the DPA Panel or an alternative dispute resolution provider based in the EU or in the U.S. Organizations that wish to cover human resources data must use the DPA Panel. • If a case is not resolved by any of the aforementioned, other means invoke binding free of charge arbitration. • Lodge a complaint to the DoC. U.S. authorities, in particular DoC, Department of Transportation (DoT) and Federal Trade Commission (FTC), may still act on their own initiative to enforce or ensure compliance.	
Relating to U.S. national security access to data	
New two-layer redress mechanism 1. Lodge complaint to the Civil Liberties Protection Officer in the Office of the Director of National Intelligence (ODNI CLPO). • For submitting a request, individuals do not need to demonstrate that their data was collected by U.S. intelligence agencies. • Complaints can be submitted through the national DPA and passed to the U.S. authority via the European Data Protection Board (EDPB). 2. Appeal before the Data Protection Review Court (DPRC).	Ombudsperson mechanism • Requests could be submitted through the national DPA and passed to the ombudsperson, who was a senior official within the U.S. Department of State. • For submitting a request, individuals did not need to demonstrate that their data was collected by U.S. intelligence agencies. • Ombudsperson investigated and then submitted a response confirming that the relevant U.S. laws had been complied with or, if the laws had been violated, the situation had been remedied. The response did, however, neither confirm nor deny whether a complainant was a target of surveillance nor did it confirm the specific remedy that was applied.

New privacy framework certification vs previous privacy shield certification

Individuals' rights	
Rights have remained the same. Individuals may obtain (i) access to, (ii) rectification of, (iii) amendment to, or (iv) deletion of personal data; and (v) limit or object to processing.	
Safeguards	
Same obligation to protect data and ensure privacy as laid out in the Principles, including purpose limitation and security measures.	
• Enhanced safeguards applying to the processing of special categories of data (sensitive information) and human resources data. • U.S. intelligence agencies' activities and obligations are governed by the Executive Order on Enhancing Safeguards for United States Signals Intelligence Activities (EO 14086), which is complemented by a U.S. Attorney General Regulation (28 CFR Part 201). • EOs carry more force than PPDs and cannot be secretly repealed as U.S. law stipulates a publication requirement. • Enhanced limitation of U.S. intelligence agencies' activities to what is necessary and proportionate, and oversight.	• Safeguards applying to the processing of special categories of data (sensitive information) and human resources data. • U.S. intelligence agencies' activities and obligations were governed by Presidential Policy Directive 28 regarding signals intelligence activities (PPD-28).
Certification process	
Similar certification procedure for new certifications. Confirm eligibility (U.S. legal entities subject to jurisdiction of FTC or DoT). • Develop conforming privacy policy. • Identify independent recourse mechanism. • Compile required information and documentation (a list is available here), such as verification of DPF commitments. • Initial self-certification and annual recertification with the International Trade Administration (ITA), DoC, via online tool, and payment of processing fee. • Certified organizations are listed in a public registry (Data Privacy Framework List) and benefit from the DPF, meaning they may receive data under the DPF from the date they are placed on this list. Note that for those already with a DPS certification, there will be an automatic conversion to DPF certification if no withdrawal. Privacy policies must be updated by October 10, 2023.	



New privacy framework certification vs previous privacy shield certification

Certification process	
More detailed submission required, which must be made by an individual within the organization who is authorized to make representations on behalf of the organization and any of its covered entities, must include the following information: • Name of the organization, as well as name(s) of any of its U.S. entities or U.S. subsidiaries that should be covered. • Contact office within the organization for the handling of complaints, access requests and any other issues arising under the Principles, including: 1. name(s), job title(s), email address(es), and telephone number(s) of the relevant individual(s) or relevant contact office(s) within the organization; and 2. the relevant U.S. mailing address for the organization. Withdrawal from the DPF is also more detailed: • DoC must be notified in advance of the wish to withdraw. • This notification must indicate what the organization will do with the personal data received in reliance upon the DPF (i.e., retain, return, or delete the data). • An organization that wants to retain such data must either affirm to the DoC on an annual basis its commitment to continue to apply the Principles or provide adequate protection by another authorized means; otherwise, the organization must return or delete the information. Corporate status change: • 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 DoC 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 DPF through an existing self-certification; (ii) self-certify as a new participant in the DPF (e.g., where the new entity or surviving entity does not already have an existing self-certification through which it could participate in the DPF); or (iii) put in place other safeguards that will ensure continued application of the Principles; otherwise any personal data received under the DPF must be promptly returned or deleted.	Submissions had to include the following information: • Name of organization, mailing address, email address, telephone and fax numbers. • Contact office for the handling of complaints, access requests and any other issues arising under the DPS. Withdrawal from the DPS: • An organization that withdrew but wanted to retain data received in reliance upon the DPS had to affirm to the DoC on an annual basis its commitment to continue to apply the Principles, or had to provide adequate protection for the information by another authorized means; otherwise, the organization had to return or delete the data. Corporate status change: • An organization that ceased to exist as a separate legal entity as a result of a merger or a takeover had to notify the DoC of this in advance. • This notification should have also indicated whether the entity resulting from the change in corporate status would (i) continue to be bound by the Principles by the operation of law governing the takeover or merger; (ii) elect to self-certify; or (iii) put in place other safeguards that would ensure adherence to the Principles; otherwise any personal data acquired under the DPS had to be deleted.
Privacy policies	
• Similar privacy policy requirements: Privacy policies must comply with the notice principle and state that the organization adheres to the Principles. • Accordingly, privacy policies must include a hyperlink to the DoC's DPF program/Data Privacy Framework List website and to the website or complaint submission form of the dispute resolution mechanism that is available.	
• An organization self-certifying for the first time may not claim DPF participation in its final (e.g., published where applicable) privacy policy until notified by the DoC that it may do so: An organization has to submit as part of the initial self-certification a draft privacy policy that is consistent with the Principles. Once the DoC has determined that the organization's initial self-certification is otherwise complete, the DoC will notify the organization that it should finalize (e.g., publish where applicable) its DPF-consistent privacy policy. The organization must promptly notify the DoC as soon as the relevant privacy policy is finalized, at which time the DoC will place the organization on the Data Privacy Framework List.	