EU – U.S. Data Privacy Framework FAQs

Authors: Julia Jacobson, Alan Friel, Sasha Koisse

Last updated: September 18, 2023

I. BACKGROUND ON DPF

Your Question	Our Answer
1. What are Privacy Shield and Safe Harbor?	The Privacy Shield was an agreement between the EU, Switzerland and U.S. under which U.S. businesses could earn a certification that allowed them to lawfully transfer personal data from the EU to the U.S. and/or Switzerland to the U.S. From August 1, 2016 until Privacy Shield was invalidated in July 2020, more than 5,000 U.S. businesses relied on their Privacy Shield certifications to lawfully transfer personal data from the EU and/or Switzerland to the U.S. Privacy Shield 'passed' three annual reviews by the European Commission but was invalidated on July 16, 2020 by the CJEU in its judgment in Case C-311/18, known as *Schrems II*. In *Schrems II*, the CJEU ruled that U.S. laws (including FISA Section 702) that enable U.S. government regulators to access signals intelligence (which includes personal data of non-U.S. persons) for national security and counter-terrorism purposes do not adequately respect and protect the fundamental privacy rights of DPF Covered Individuals when their personal data is transferred to the U.S. In particular, the CJEU noted the lack of an effective judicial redress process in U.S. courts for EU citizens. Privacy Shield's invalidation was declared almost four years to the date after a joint EU-U.S. statement announced its validation on July 12, 2016. Like its successor, the Safe Harbor Framework (***Safe Harbor***) was an agreement between the EU and U.S. through which U.S. businesses could earn a certification that allowed for the lawful transfer of personal data from the EU to the U.S. The CJEU's judgment in Case C-362/14, known now as "***Schrems I***," invalidated the Safe Harbor on October 6, 2015. Like the *Schrems II* judgment, the CJEU's decision in *Schrems I* noted (among other issues) the U.S. law permitting U.S. public authorities access on "a generalized basis to the content of electronic communications" on non-U.S. persons. After ten months of negotiation, the Privacy Shield became operational on August 1, 2016, to replace Safe Harbor. Privacy Shield's main differences compared to Safe Harbor were stricter requirements for ***onward transfers*** of personal data (i.e., transfers of personal data from a certified business to a third party controller or processor) and commitments by the DoC and U.S. Federal Trade Commission (***FTC***) to monitor and enforce compliance more actively. The other main difference is that, for unresolved privacy complaints made by

Subscribe By Email

Your Email Address

Subscribe

Litigators +

Compliance Advisors +

Stay Connected

Topics

Select Category

Archives

Select Month

Recent Posts

You have Questions, We have Answers: Data Privacy Framework FAQs

China Releases Draft Regulation to Significantly Ease Cross-border Data Transfers

Privacy World Week in Review

Fewer Clouds on ... Cloud: The EU to (Finally) Drop Most Data Localisation Requirements in the EUCS

Join us on September 28 for a Webinar on Washington's My Health My Data Act and other Consumer Health Data Regulation

	an DPF Covered Individual, an arbitration right and redress mechanism were included, which enabled the DPF Covered Individual to learn whether the complaint was investigated and receive redress for non-compliance.
2. What is an "adequacy decision"?	The European Commission defines an adequacy decision as: "one of the tools provided under the [GDPR] to transfer personal data from the EU to third countries which, in the assessment of the [European] Commission, offer a comparable level of protection of personal data to that of the European Union. As a result of adequacy decisions, personal data can flow freely and safely from the European Economic Area (EEA) … to a third country, without being subject to any further conditions or authorisations … In other words, transfers to the third country can be handled in the same way as intra-EU transmissions of data…" The list of jurisdictions that are subject to an EU adequacy decision is available online[1]. FADP has a similar list of jurisdictions[2]. For the UK GDPR, the ICO (the UK privacy regulator) issued a list of jurisdictions that are subject to a UK adequacy decision.[3]
3. Who or what is "Schrems"?	Max Schrems, the plaintiff in both *Schrems I* and *Schrems II*, is an Austrian privacy activist. Mr. Schrems started his legal battle by asking the Irish data protection regulator to investigate whether Facebook's transfer of his personal data from Facebook Ireland to Facebook Inc. by way of Facebook's Safe Harbor certification was lawful under EU privacy laws. Fueled by Edward Snowden's 2013 release of classified documents detailing U.S. counter-terrorism surveillance activities, Mr. Schrems alleged that his EU data protection rights were violated by U.S. intelligence agencies' ability to access his personal data after it was transferred to Facebook in the U.S. The Irish data protection regulator ultimately referred Mr. Schrems case to the CJEU which agreed with Mr. Schrems and invalidated Safe Harbor. As noted above, Mr. Schrems' challenge to Privacy Shield in *Schrems II* also was successful. Mr. Schrems already has announced his intention to challenge the DPF.
4. How is DPF different from Privacy Shield?	The primary change between Privacy Shield and DPF is a change in U.S. law. Last October, President Biden issued an Executive Order that formalized the U.S. commitment to ensure that signals intelligence activities are necessary and proportionate in the pursuit of defined national security objectives and create a new mechanism for individuals to seek redress if they believe they are unlawfully targeted by signals intelligence activities. The Executive Order also created a multi-layer mechanism for these individuals to obtain review and redress of claims that their personal data collected through U.S. signals intelligence was collected or handled in violation of applicable U.S. law. The DPF also provides for a more robust redress mechanism for pursuing complaints of non-compliance with the DPF requirements. This enhanced redress mechanism includes seven options starting with lodging a complaint with the DPF certified business up to redress in U.S. courts.
5. What is the Swiss DPF?	The Swiss DPF is the data transfer mechanism that U.S. regulators expect that the Swiss Federal Administration will recognize by issuing an adequacy decision under the Federal Act on Data Protection of Switzerland (***FADP***). Once the adequacy decision under FADP is issued, a certified business participating in the Swiss DPF can receive Swiss personal data in the United States in compliance with Swiss law. Although U.S. regulators expect the FADP adequacy decision, Switzerland's Federal Data Protection and Information Commissioner

	(***FDPIC***) announced that, as of September 1, 2023, "Switzerland's adequacy list will remain unchanged" until the Swiss Federal Council issues that adequacy decision. In other words, U.S. businesses can certify to the Swiss DPF but cannot yet rely on it for personal data transfer from Switzerland to the U.S.
6. Does the UK have a Data Privacy Framework?	No. In June, the U.S. and UK agreed in principle to establish the UK Extension to the Data Privacy Framework – also known as the 'data bridge.' The UK Extension provides a mechanism for UK to U.S. personal data transfers in compliance with the UK GDPR. The UK Extension also will apply to personal data transfers from Gibraltar. A DPF-certified business can choose to add the UK Extension to its EU DPF certification but cannot certify to the UK Extension independently. In other words, a U.S. business can certify to the EU DPF and/or the Swiss DPF but the business can only add the UK Extension if it already has received the EU DPF certification. As this time, whether the UK and Swiss governments will reach a similar agreement for a data bridge for the Swiss DPF is unknown.
7. What are the DPF Principles and how are they different from the requirements in the U.S. state privacy laws?	The seven core DPF Principles are as follows: **(1) Notice**: The ***DPF Notice Principle*** requires a certified business to inform individuals whose personal data is covered by DPF (***DPF Covered Individuals***) about their rights and the certified business' obligations under DPF. The certified business must provide the notice at the time of personal data collection or "as soon thereafter as is practicable." Supplemental Principle 9 includes additional obligations for ***HR Data***, personal data about past and present employees (who are DPF Covered Individuals) collected in the context of the employment relationship. *U.S. State Laws*: The notice requirements under DPF are like the several pre-processing notice requirements under the U.S. state privacy laws. The DPF however covers personal data collected from or about employees and customers (whether B2B or B2C) and other non-employee DPF Covered Individuals, each of whom is in the EEA and UK and/or Switzerland, if applicable. Like the U.S. state privacy laws, the DPF notice for non-HR Data must be published on the certified business' publicly available website, but the business may choose whether to post the DPF notice for HR Data on its publicly available website. Supplemental Principle 9b provides additional information about application of the Notice Principle to HR Data, emphasizing that nothing in DPF is meant to supersede restrictions in European law related to employee personal data processing. See Section VI below for more information about the content requirements for DPF notices. **(2) Choice**: The ***DPF Choice Principle*** requires a certified business to offer certain choices to DPF Covered Individuals whose personal data is received by the business under DPF. These choices are the opportunity to **opt out** of: • the disclosure of their personal data to another ***Controller*** (i.e., an organization that, alone or jointly with others, determines the purposes and means of the processing of personal data); • the use of their personal data for a purpose that is materially different from the purpose(s) for which the personal data was originally collected (as described in the relevant notice) or subsequently authorized by the DPF Covered Individuals; and • having personal data used for direct marketing. This direct marketing opt-out right is "subject to reasonable limits" established by the certified business, such as "time to make the opt out effective" (see Supplemental Principle 12). A certified

business also may use the personal data 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."

Supplemental Principle 9b provides additional information about application of the Choice Principle to HR Data emphasizing that nothing in DPF is meant to supersede restrictions in European law related to employee personal data.

U.S. State Laws: The choices offered under the DPF Choice Principle are like the privacy rights available under the U.S. state privacy laws but, of course, the DPF choices are available to DPF Covered Individuals rather than residents of the specific states that have passed privacy laws. Accordingly, depending on how the certified business currently handles U.S. state privacy rights and GDPR data subject rights, DPF compliance may require some changes or additions to current processes. See Access Principle (below).

For "sensitive information," the certified business must obtain the DPF Covered Individual's "affirmative express consent" before disclosing the sensitive information to a third party or before using the sensitive information for a purpose not covered in the original notice or authorized by the affirmative express consent. In Principle 2 (Choice), ***sensitive information*** is defined as medical or health conditions, race or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership and sex life information. Supplemental Principle 1a (which uses the term "sensitive data" instead of sensitive information) lists exceptions to the affirmative express consent requirement. See Section VI below for more information.

U.S. State Laws: the California Consumer Privacy Act (California's state privacy law known as ***CCPA***) requires opt-out consent to sensitive personal information processing (as does the Utah state privacy law) but the state privacy laws in Colorado, Connecticut, Utah and Virginia require opt-in consent for sensitive personal information processing.

The DPF's definition of sensitive information in Principle 2 is narrower than the definition under GDPR Article 9[4]. But the DPF Adequacy Decision states that "any data that is considered sensitive under Union data protection law (including data on sexual orientation, genetic data and biometric data) will be treated as sensitive under the EU-U.S. DPF by certified organisations" (Clause 18).

U.S. State Laws: the U.S. state privacy laws in Connecticut, Utah and Virginia include precise geolocation in the sensitive personal information category. CCPA and the U.S. state privacy laws in Connecticut and Virginia include personal data collected from a known child. CCPA § 1798.140(ae) also is arguably broader than GDPR Art. 9 by including precise geolocation and contents of a consumer's mail, email and text messages (unless the business is the intended recipient of the communication) but the CCPA definition does not include "political opinions."

(3) Accountability for Onward Transfers: DPF requires a certified business to comply with certain procedures and impose certain types of contractual terms when transferring personal data received from the EU (and UK and/or Switzerland).

	Unlike GDPR, a Controller-to-Controller transfer requires a contract under Supplemental Principle 10c. Existing data processing agreements that rely on Standard Contractual Clauses (***SCCs***) are not sufficient under DPF because they do not address the DPF Principles. Accordingly, a certified business should review and update data processing agreements that apply to personal data transfer to the U.S. under DPF. **(4) Security**: Similar to GDPR Art 32, DPF requires taking reasonable and appropriate measures to protect personal data from loss, misuse and unauthorized access, disclosure, alteration and destruction while taking into due account the risks involved in the processing and the nature of the personal data. *U.S. State Laws*: Like the U.S. state data security and state privacy laws, a DPF certified business that collects personal data must implement reasonable security procedures and practices appropriate to the nature of the personal data to protect the personal data from unauthorized or illegal access, destruction, use, modification or disclosure. **(5) Data Integrity and Purpose Limitation**: DPF generally requires a certified business to use and retain personal data only for the purposes for which it has been collected or subsequently authorized by the DPF Covered Individual. DPF also requires taking reasonable steps to ensure the reliability of personal data with respect to its intended use. **(6) Access**: Subject to some exceptions and exemptions, DPF requires a certified business to allow DPF Covered Individuals to access their personal data. DPF also generally requires allowing DPF Covered Individuals to correct, amend, or delete personal data deemed inaccurate or processed in violation of DPF. Supplemental Principle 8 includes details about how to operationalize the Access Principle, such as when a business can deny or limit access and when a certified business may charge a fee for providing access. Supplemental Principle 9 explains that, for HR Data, the certified business is expected to cooperate with EU employers. **(7) Recourse, Enforcement, and Liability**: DPF requires a certified business to implement robust recourse mechanisms, cooperate with authorities, and arbitrate claims in accordance with DPF. Additional requirements apply when self-certifying to DPF for HR Data. Supplemental Principle 11 sets out additional details for Dispute Resolution and Enforcement. See Section V below for more details. *U.S. State Laws*: Like the U.S. state privacy laws, which provide that publicly available information is not included in the definition of "Personal Data," the DPF provides that it is not necessary to apply the Notice, Choice, Access, or Accountability for Onward Transfers Principles to public record information, if all conditions established by relevant jurisdictions are met. The Notice, Choice, Access, or Accountability for Onward Transfers Principles must be applied, however, when the public record information is combined with non-public record information. It is also not required to apply the Notice, Choice, or Accountability for Onward Transfers Principles to publicly available information unless the transferor indicates that the publicly available information is subject to restrictions that require application of the Principles for the intended uses of the DPF certified business.
8. Does certification mean that a DPF-certified business is compliant with	No. The DPF is the result of an adequacy decision under Article 45 of the GDPR. It does not address other compliance GDPR obligations.An adequacy decision does not mean that the privacy law that is covered by

the GDPR?	the adequacy decision is identical to GDPR; rather the privacy law is deemed to have "essential equivalence."For example, the DPF requires the certified business to:
	• Provide **prior notice** about personal data processing under the DPF Notice Principle, which is similar to GDPR Art. 13-14.
	• Allow EU citizens the **right to choose**:
	  • whether the certified business can use their personal data for a materially different purpose than was originally disclosed under the DPF Choice Principle – like GDPR Art 18 (which is broader)).
	  • whether the certified business can disclose their personal data to a third party (other than an ***Agent*** (i.e., a **t**hird party acting on behalf of a DPF certified business that is a **C**ontroller (aka processor)) of the certified business (DPF Choice Principle), which is similar to the requirements in GDPR Art 7, 18.
	• Obtain **express opt-in consent** (like GDPR Art 9) before sensitive personal data is disclosed to a third party or used for a different purpose than the purpose for which it was originally collected (DPF Choice Principle), subject to some limited exceptions described in Supplemental Principle 1.
	• Only collect personal data that is relevant for the specific purposes disclosed in the DPF privacy policy and not use personal data for a new or different purpose unless and until affected DPF Covered Individuals receive supplemental notice about the new or different purpose and authorize the new or different uses (DPF Data Integrity and Purpose Limitation Principle), which is like GDPR Art 5(1)(b)).
	• Use reasonable efforts to ensure that personal data is accurate, complete and current for its intended processing purposes (DPF Data Integrity and Purpose Limitation Principle), which is similar to GDPR Art 5(1)(d)).
	• Retain personal data only as long as necessary for the purpose of processing (DPF Data Integrity and Purpose Limitation Principle and GDPR Art 5(1)(b)).
	• Protect personal data from unauthorized processing (DPF Security Principle and GDPR Art 5(1)(f)). (The U.S. data breach notifications in all 50 states still will apply as to data breaches.)

9. What are the benefits of DPF certification?	DPF certification reduces the administrative compliance obligations on a certified business transferring personal data to the U.S. from the EU and, when applicable, Switzerland and the UK. Once certified, a business does not need SCCs with data exporters to the U.S. for personal data transfers from EU, Switzerland and/or UK. In other words, the certified business does not need to execute SCCs with each customer, vendor or business partner involved in these cross-border transfers and can have somewhat more flexibility in contacting because by avoiding the need to use the terms of the SCCs verbatim. (Many businesses may, however, wish to retain or enter into SCCs for ongoing personal data transfers just in case DPF suffers the same fate as its predecessors. And, transfers of personal data to any other jurisdiction not subject to an adequacy decision still require SCCs or another lawful mechanism under GDPR.) DPF certification also means that, for EEA to U.S. personal data transfers, a certified business can dispense with TIAs, used for analyzing the impact on privacy when personal data is transferred from the EEA to a jurisdiction outside of the EEA that is not deemed 'adequate' by the European Commission. Many certified businesses will realize significant costs savings from reducing the use of SCCs and TIAs for DPF-covered transfers. For businesses without an EU location, the DPF minimizes some of the difficulties arising from GDPR's extra-territorial scope. That is, for a

	certified business subject to GDPR because of GDPR Art 3(2), the DPF allows transfers of personal data collected in the EU directly to the U.S. without the need for a data exporter under the SCCs. The DoC notes that the DPF's compliance obligations are "clearly laid out" (as compared to EU, UK and Swiss data protections laws), which clarity benefits small and medium sized businesses.
10. What is the likelihood that the DPF will be challenged in court like the Privacy Shield Framework?	The DPF already was challenged by the European Center for Digital Rights, a non-profit organization founded by Max Schrems (see Part 1, FAQ 2) and known colloquially as NOYB. In a press release issued on July 10, 2023 (the same day on which the EU Commission announced the DPF adequacy decision), NYOB announced its readiness to challenge the DPF for inadequately addressing the EU's concerns about government surveillance and redress for individuals. On September 7, 2023, Philippe Latombe, a member of the French National Assembly, announced that he is challenging DPF in his "personal capacity". In his press release, Latombe stated that the DPF text was not subject to informed debate by the European Parliament and violates the Charter of Fundamental Rights of the Union by providing "insufficient guarantees of respect for private and family life". Latombe requests the immediate suspension of DPF and replacing DPF with a more "balanced" framework. In the meantime, however, EU organizations and certified businesses can take advantage of the DPF to receive personal data in the U.S.

II. ELIGIBILITY FOR DPF CERTIFICATION

Your Question	Our Answer

1. What businesses are eligible for DPF Certification?	Broadly, the DPF is available for U.S. legal entities that are subject to the investigatory and enforcement powers of the FTC or the U.S. Department of Transportation (***DoT***).
	
	The Federal Trade Commission Act (***FTC Act***) grants the FTC broad authority over acts or practices affecting interstate commerce by any person, partnership or corporation. Generally, this means **businesses operating for profit in the U.S.**
	
	• The FTC does not have authority over:
	  ◦ "most" depository institutions (banks, federal credit unions, and savings & loan institutions),
	  ◦ telecommunications and interstate transportation common carrier activities (see also FAQ II.4 below).
	  ◦ air carriers
	  ◦ labor associations
	  ◦ "most" packer and stockyard activities.
	• As noted on the DPF Website, the FTC's jurisdiction over insurance activities "is limited to certain circumstances".
	• The DPF Website also states that the FTC does not have authority over "most non-profit organizations".
	  ◦ The FTC Act (15 U.S. Code § 44) defines "corporation" as any company, trust, so-called Massachusetts trust, or association, incorporated or unincorporated, which is organized to carry on business **for its own profit or that of its members.**" Accordingly, the FTC does not have authority over not-for-profit (or tax-exempt) charitable corporations. But, the FTC will exercise its authority if tax-exempt charitable organization is misusing its funds or if the organization's status as a charitable organization is a sham. Also, most trade and professional associations that are tax-exempt under Section 501(c)(6) of the Internal Revenue Code are subject to the FTC's jurisdiction.

2. Are healthcare organizations eligible for DPF Certification?	Covered entities and business associates operating *for-profit* under the federal Health Insurance Portability and Accountability Act of 1996 (***HIPAA***) are eligible for DPF certification. U.S. businesses that collect, use and share health-related personal data – or HIPAA-adjacent health information [5] – that is outside the scope of HIPAA are subject to FTC oversight. The application of DPF to businesses engaged in medical or pharmaceutical research studies is discussed in Supplemental Principle 14. Several businesses that process health-related information already received DPF certification, including, for example: 23andMe, Inc., Acadia Pharmaceuticals, Cerner Corporation, Flo Health, Inc., New England Research Institutes, Inc. and Precision Digital Health.
3. Are professional associations eligible for DPF Certification?	Most trade and professional associations – including associations that are tax-exempt under Section 501(c)(6) of the Internal Revenue Code – are subject to the FTC's jurisdiction and eligible for DPF certification.
4. Are FCC-regulated entities eligible for DPF Certification?	Entities regulated by the Federal Communications Commission (***FCC***) are eligible for DPF certification to the extent that they also are subject to FTC jurisdiction. FCC-regulated entities, including telecommunications carriers, are outside of FTC jurisdiction if they are engaged in "common carrier" activities. Common carrier activities include entities engaged as a common carrier for hire, by wire, radio, or interstate or foreign radio transmission, including landline and wireless telephone services and commercial mobile services. If FCC-regulated entities engage in non-common carrier activities, they are subject to FTC authority (see *Federal Trade Commission v. AT&T Mobility LLC*.) Accordingly, FCC regulated entities engaged in non-common carrier activities are eligible for DPF certification. This includes landline and wireless telephone services, as well as commercial mobile services. Relatedly, broadband internet access services, or ***BIAS***, are no longer common carriers. In 2018, the FCC re-classified BIAS as a type of "information service" rather than a "telecommunications service." BIAS also includes mobile broadband, which is high-speed internet access delivered to mobile devices.

III. PERSONAL DATA TRANSFERS COVERED BY DPF

Your Question	Our Answer
1. Does DPF means that the U.S. has received an adequacy jurisdiction?	No. The European Commission's DPF adequacy decision only applies to certified businesses for personal data transfers from an organization in the EEA to a certified business. Likewise, when the governments of the UK and Switzerland approve their respective adequacy decisions, the DPF will apply to personal data transfers from any organization in the UK and/or Switzerland to certified businesses under the UK Extension and/or Swiss DPF.
2. Does the DPF apply to all personal data or only certain categories of personal data?	The DPF certification applies to personal data transferred to the U.S. from EU and, once applicable, Switzerland and UK. Certifying businesses can choose whether to certify for: • HR Data; and/or • non-HR Data (e.g., personal data collected from or about a customer, client, website visitor). Presumably, personal data collected from applicants and independent contractors is covered as non-HR Data.

3. Does DPF apply to transfer of personal data from the EEA or the EU only?	Yes. DPF covers transfers from the 27 EU member states and Norway, Iceland and Liechtenstein. See FAQ I.5 and FAQ I.6 for more information.
4. Are transfers from other countries subject to an EU adequacy decision covered by DPF?	No. Although the EU has issued adequacy decisions (see FAQ I.8) for Andorra, Argentina, Canada (commercial organisations only), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea and Uruguay, they are not currently participating in the DPF. As noted above, only personal data transfers from EEA and, once approved, UK and Switzerland are covered by the DPF.
5. At which point in the data transfer lifecycle does the DPF apply?	The DPF applies to personal data transferred from the EEA (or, when in force, the UK Extension and Swiss DPF) to a certified business. The application of the DPF is not time-limited: certified businesses must continue to apply the Principles to personal data for as long as the certified business processes the personal data, even if the certified business subsequently withdraws from or is removed from the DPF for any reason. The certified business also must ensure that the DPF applies to all personal data received by it in the U.S. that the certified business subsequently transfers.

IV. DPF CERTIFICATION FEES AND COSTS

Your Question	Our Answer
1. How much does DPF certification cost?	DPF certification requires the following fees:1. Certification Fee. DPF certification requires payment of an annual certification fee to the International Trade Administration (***ITA***). The annual fee is tiered based on each certified business's annual revenue, as follows: • **$0 to $5 million**, certifying to a single framework is $250 annually, and certifying to both frameworks* is $375 annually. • Over **$5 million to $25 million**, certifying to a single framework is $650 annually, and certifying to both frameworks is $975 annually. • Over **$25 million to $500 million**, certifying to a single framework is $1,000 annually, and certifying to both frameworks is $1,500 annually. • Over **$500 million to $5 billion**, certifying to a single framework is $2,500 annually, and certifying to both frameworks is $3,750 annually. • Over **$5 billion** certifying to a single framework is $3,250 annually, and certifying to both frameworks is $4,875 annually.* The UK Extension does not require additional fees. 2. Annual Fees for the Arbitral Fund. The arbitral fund covers the fees associated with the DPF Panel (see FAQ V.1 below) **Data Privacy Framework Arbitral Fund Fee Schedule** ***Approved by the U.S. Department of Commerce on August 5, 2017*** | Participating Organization Annual Revenue | Required Contribution | |---|---| | $0 to $5 million | $250 | | Over $5 million to $25 Million | $500 | | Over $25 million to $500 million | $1,000 | | Over $500 million to $5 billion | $5,000 | | Over $5 billion | $10,000 | 3. Fees for an Independent Recourse Mechanism (***IRM***) – IRM fees apply for both HR Data and non-HR Data. The IRM fees for non-HR Data vary by IRM provider. (See FAQs V. 2 and V.3 below.) For HR Data, the business must commit to cooperate with the appropriate European data protection authority/ies for the relevant part(s) of the DPF program, i.e., the EU data protection authorities (***EU DPAs***) under the EU-U.S. DPF; the UK Information Commissioner's Office

	(***ICO***) and, as applicable the Gibraltar Regulatory Authority (***GRA***) under the UK Extension to the EU-U.S. DPF; or the Swiss FDPIC under the Swiss DPF (collectively, the ***DPA Panel***). That is, the DPA Panel is the only permitted IRM provider for HR Data. The fee for the DPA Panel is $50 per year which covers EU DPF and UK Extension and the Swiss DPF.
2. Does a business with an active Privacy Shield certification need to pay the same fees?	A business that maintained an active certification under the Privacy Shield is automatically part of DPF – as long as the business' privacy policies and procedures are updated to reflect the Principles by October 10, 2023 and by October 17, 2023 for the Swiss DPF. The business will need to re-certify on its annual re-certification date and pay the IRM(s) and Arbitral Fund annual fees.
3. Is a business with a lapsed or withdrawn Privacy Shield certification eligible for the abbreviated DPF certification? Does it depend on how long since the Privacy Shield certification lapsed or was withdrawn?	The DPF Website is not entirely clear on this point. We assume, however, that the answer is no, a business that withdrew from Privacy Shield must re-certify.

V. DISPUTE RESOLUTION

Your Question	Our Answer
1. How are complaints resolved under the DPF?	Under the DPF Notice Principle, a certified business must publish contact information for complaint submission and an IRM. The DPA Panel is the only IRM allowed for HR Data, but a U.S. business may choose a different IRM for non-HR Data. Contacting an IRM is either the first or second step in the process for complaint resolution. If the DPF Covered Individual reaches out to the certified business first, then the certified business must respond to the complaint no later than 45 days after receiving the complaint. The aggrieved DPF Covered Individual can choose to utilize the IRM as a first step, although an IRM is expected to encourage contacting the certified business first. The IRM can award monetary damages, injunctive relief and impose sanctions, which "should include publicity for findings of non-compliance and the requirement to delete data in certain circumstances" (Supplemental Principle 11.e). The DPF Covered Individual also can reach out to an EU DPA when HR Data is involved or if the certified business voluntarily agrees to submit to the EU DPA's oversight. (If a DPF Covered Individual otherwise reaches out to an EU DPA in any other case, then the EU DPA is expected to refer the DPF Covered Individual to the DoC or FTC.) If the certified business does not comply with the EU DPA's "advice," then the EU DPA can refer the complaint to the DoC. The DoC can remove the certified business from the DPF Active list or refer the case to the FTC or DoT, as applicable (see FAQ II.1 above). If the complaint that a certified business has violated its DPF obligations remains unresolved after all of the above options are exhausted, then the next step is an arbitration option known as the EU-U.S. Data Privacy Framework Panel (***DPF Panel***). The DPF Panel is comprised of up to three arbitrators agreed by the parties selected from a pool of arbitrators designated by the DoC and European Commission. The International Centre for Dispute Resolution administers the arbitrations. The DPF Panel only has the authority to

	impose "individual-specific, non-monetary equitable relief (such as access, correction, deletion or return of the individual's data in question)" (DPF Annex I). The individual also can bring the action to a U.S. court, such as for violation of state consumer protection laws (when a private right of action is available) or for privacy related torts.
2. What is an independent recourse mechanism (IRM) and what does it do?	An IRM is intended to ensure compliance with the DPF by allowing a DPF Covered Individual to submit a complaint to an independent third party that can investigate and resolve the DPF Covered Individual's complaints at no cost to that individual. The DPF requires that IRMs are impartial and transparent. An IRM must: • Provide covered DPF Covered Individuals with information about the DPF and how to file a complaint, timing for processing complains, a description of potential remedies and a notice about the IRM's privacy practices • Investigate and expeditiously resolve each complaint received • Publish an annual report that includes aggregate statistics regarding the dispute resolution services. IRMs can also award damages for those affected by noncompliance. If the IRM does not resolve the DPF Covered Individual's complaint, that individual also may choose binding arbitration by the DPF Panel (see FAQ V.6 below). The DoC is responsible for verifying that IRMs meet DPF requirements.
3. How do we choose an IRM?	Current options for personal data that is not HR Data: • Better Business Bureau – Form • JAMS – here • TRUSTe – here • International Centre for Dispute Resolution-American Arbitration Association (ICDR-AAA) – program information • PrivacyTrust – Apply online • VeraSafe – Enroll online • Insights Association – Form • The ANA – Webpage
4. How does a non-U.S. citizen raise concerns about U.S. intelligence access for national security and surveillance purposes to their personal data transferred to the U.S.?	By Executive Order (***EO***) issued on October 7, 2022, President Biden authorized the Director of National Intelligence to create a multi-layer mechanism for non-U.S. individuals to obtain review and redress of claims that their personal data collected through U.S. signals intelligence was collected or handled by the U.S. in violation of applicable U.S. law. Under the first layer, the Civil Liberties Protection Officer in the Office of the Director of National Intelligence (***CLPO***) will conduct an initial investigation of qualifying complaints received to determine whether the EO's enhanced safeguards or other applicable U.S. laws were violated and, if so, to determine the appropriate remediation. As a second layer of review, the Data Protection Review Court (***DPRC***) created by the U.S. Attorney General provides an independent and binding review of the CLPO's decisions upon an application from the individual or an element of the Intelligence Community. The EO also requires an annual review of the redress process, including whether the Intelligence Community has fully complied with determinations made by the CLPO and the DPRC. (See also FAQ I.3.)
5. What is outside compliance reviewer and what does it do?	The DPF contemplates that approved outside compliance vendors may be used as an alternative to self-certification, although the DoC has yet to approve any. Many IRMs, like the BBBNP played a similar role under Privacy Shield and expect to do so under DPF. However, this service is

	separate from IRM services.

VI. DPF POLICIES AND PROCEDURES

Your Question	Our Answer
1. What policies do we need for DPF?	The DPF requires a DPF-compliant privacy policy for HR Data and for non-HR Data. The DPF website provides sample provisions for explaining certification to the two Frameworks and UK Extension; the authority of the FTC and/or DoT as to DPF; and the internal complaint process. The DPF also has compliance and recordkeeping obligations that we recommend adding to existing internal policies and procedures or to DPF-specific policies and procedures. The covered business must (inter alia) ensure that employees are trained on the implementation of the DPF and conduct periodic compliance reviews or manage the requirements of the outside compliance reviews and cover honoring DPF choice and access requirements and tracking opt-in/opt-out consent and affirmative consent for sensitive information.
2. Do we need a separate DPF privacy policy or can the business incorporate DPF-specific notice requirements into its existing privacy policy?	The DPF does not require separate policies. A certified business can include required DPF disclosures in an existing privacy policy and/or can cover both HR Data and non-HR Data in a single privacy policy. In each case, the DPF Notice Principle requires that the certified business provide its privacy policies in clear and conspicuous language when individuals are first asked to provide the personal data or as soon as practicable thereafter, but in any event before the data is used for a materially different (but compatible) purpose than the one for which it was collected, or before it is disclosed to a third party.
3. How are the privacy policies for HR Data and non-HR Data different?	For HR Data, the DPF does not require publicly posting the privacy policy but, for non-HR Data, the certified business must post the privacy policy on its website or otherwise provide information about where the privacy policy is available for the general public to access. As noted in FAQ V.1, the certified business must cooperate with the DPA Panel as the IRM. The DPF also requires employers to accommodate the privacy preferences of employees by restricting access to HR Data, anonymizing certain HR Data or assigning codes or pseudonyms. Supplemental Principle 9 explains how the Notice and Choice Principles apply specifically to HR Data. Generally, a certified business must abide by the Notice and Choice Principles when disclosing HR Data to third parties or using it for a different purpose than originally contemplated. However, the Notice and Choice Principles do not need to be provided if it is necessary to avoid prejudicing the ability of a certified business to make promotions, appointments, or other similar employment decisions. This is a broad exception to Notice and Choice for HR Data.

VII.

Your Question	Our Answer
1. Do I need to update a data processing agreement designed for GDPR, UK GDPR and/or FADP (together, *European Privacy Laws*)?	In DPF, a processor is also referred to as an "agent". European Privacy Laws – such as GDPR Art 28 – generally require an agreement between a controller and processor. No additional authorization is required when a certified business is merely processing personal data because the DPF deems the certified business to provide adequate protection.
2. Do I need a controller-to-controller data processing agreement?	Yes, when a certified business shares personal data covered by DPF with another controller, the certified business must enter into a data processing contract to ensure that the personal data receives DPF-level protections. European Privacy Laws do not require controller-to-

	controller data processing agreements except when the SCCs apply to the personal data transfers.
3. Does a certified business have an affirmative obligation to verify a vendor's DPF certification? Is certified business liable for using a vendor that misrepresented its DPF certification status?	No. When a DPF-certified business transfers personal data to another U.S. business, the DPF does not require that the recipient U.S. business is DPF-certified. The transfer must, however, otherwise comply with DPF.

[1] Last accessed September 1, 2023.

[2] Last accessed September 1, 2023.

[3] Last accessed September 1, 2023.

[4] The DPF definition of sensitive information does not include genetic data and, biometric data which are in GDPR Article 9.

[5] See, e.g., here, and here.

Address

Squire Patton Boggs (US) LLP
555 South Flower Street
31st Floor
Los Angeles, California 90071
Phone: 213-689-6510

Contacts

Kristin Bryan | Marisol Mork | Alan Friel