Media coverage

February 2018

1. OVERVIEW

On 12 July 2016, the European Commission formally approved and adopted the EU-US Privacy Shield, providing a new compliance framework for US organisations that are involved in the importation of personal data from Europe. The Privacy Shield is one mechanism to satisfy EU requirements for adequate protection for transfers of personal data outside the European Economic Area ('EEA') to the US. Other mechanisms include, model clauses and Binding Corporate Rules. The Privacy Shield replaces its predecessor, EU-US Safe Harbor Framework, but introduces several new requirements. These include new rules for privacy policy disclosures, heightened requirements for onward transfers of personal data, and stronger redress mechanisms for data subjects.

2. CERTIFICATION

The Privacy Shield is a voluntary self-certification scheme, administered by the U.S. Department of Commerce.

2.1. Eligibility to join Privacy Shield

Certification is available to any US organisation that processes personal data in connection with an activity that is subject to the jurisdiction of the Federal Trade Commission ('FTC') or the U.S. Department of Transportation. This covers most US organisations, although generally excludes banks, federal credit unions, savings and loan institutions, telecommunications and interstate transportation common carriers, labour associations, most non-profit organisations, most organisations involved in packer and stockyard activities, and most insurance companies. Organisations that fall under these regulatory categories should seek further guidance from legal counsel before applying for the Privacy Shield. Non-US organisations (including organisations incorporated in the EU) cannot certify for the Privacy Shield, because they are not subject to the jurisdiction of either the FTC or the Department of Transportation.

2.2. Application procedures and requirements

For an organisation to certify for the Privacy Shield, it must complete the following:

2.2.1. Privacy policy

Adopt a clear, concise, and easy-to-understand privacy policy that complies with the Privacy Shield Principles ('the Principles') and provide a link to the web address where the privacy policy is available. The privacy policy (including the public version) must include the following *at the time the organisation submits its Privacy Shield application*:

a statement that the organisation adheres to the Principles;
a link to the Privacy Shield website (https://www.privacyshield.gov/); and
a link to the website or complaint submission form of the independent recourse mechanism chosen (see Section 2.2.3. below).

2.2.2. Onward transfers

Review arrangements for the onward transfer of personal data to third parties, including reviewing and updating contracts with those third parties to include certain required provisions. The requirements differ according to whether the third party will be acting as a controller or an agent (the Privacy Shield-terminology for 'processor').

For transfers to third party controllers, organisations must:

give individuals notice and the opportunity to opt out, or, in case of sensitive data (see Section 3.2. below), obtain their consent prior to the transfer; and
enter into a contract that provides that data may only be processed for limited and specified purposes consistent with the consent provided by the individual; and the third party will provide the same level of protection as the Principles, will notify the organisation if it makes a determination that it can no longer meet this obligation and, if so, cease processing or take other reasonable and appropriate remedial steps.

For transfers to third party agents, organisations must:

transfer personal data only for limited and specified purposes;
ascertain that the agent is obligated to provide at least the same level of privacy protection as is required by the Principles;
take reasonable and appropriate steps to ensure that the agent effectively processes the personal data in a manner consistent with the organisation's obligations under the Principles;
require the agent to notify the organisation 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 and, if so, take reasonable and appropriate steps to stop and remediate unauthorised processing; and
provide a summary or a representative copy of the relevant privacy provisions of its contract with that agent to the Department of Commerce upon request.

2.2.3. Independent recourse mechanism

Choose an independent recourse mechanism and register with the recourse mechanism provider, if required (see below). This is necessary to comply with the new requirement to provide a third-party investigative body to address data subjects' unresolved complaints regarding the organisation's compliance with the Principles. The recourse mechanism must be provided at no cost to data subjects. Organisations have two options for satisfying this requirement:

1. registering with a private sector privacy programme; or
2. committing to cooperate and comply directly with the EU data protection authorities ('DPAs').

If the self-certification will cover human resources data, then the organisation *must* agree to cooperate and comply with DPAs with respect to such data, i.e., must choose option two in relation to such data. Organisations choosing option two are subject to an annual fee of $50 (there is no need to register with a DPA). For organisations that chose to register with a private sector privacy programme, registration must be complete prior to submitting the

Privacy Shield application. Private sector programmes typically charge either: annual fees, ranging from $300 to $7,000 per year, (depending on the organisation's annual revenue); or a fee-per-dispute, ranging from $500 to $2250 per dispute.

2.2.4. Verification mechanism

Either register with a third-party assessment programme to verify annual compliance with the Principles; or commit to performing an internal annual assessment to verify such compliance. Most organisations chose to perform this annual compliance check themselves.

2.2.5. Other information

Provide the following additional information in the application:

> **Privacy Shield contact:** Name and contact information of the designated individual that will be responding to inquiries about the Privacy Shield, including complaints from data subjects.
> **Description of the organisation's data processing activities:** A description of the types of personal data the self-certification covers, the purposes for which the personal data is processed, and the types of third parties with whom the organisation discloses personal data.
> **Organisational entities included in the application:** A list of all US entities (affiliates and subsidiaries) within the organisation's corporate group that are adhering to the Principles and are covered under the organisation's self-certification.
> **Annual revenue:** The organisation's annual revenue (to calculate the annual fee; see section 2.2(f) below).

2.2.6. Fees

Pay the following fees, calculated by reference to the organisation's annual revenue:

> Annual Privacy Shield Fee (paid upon submission of application); and
> One-time Privacy Shield Arbitral Fund Fee for the Annex I Binding Arbitration Mechanism (this fee may be paid here).

Annual Revenue of Organisation	**Annual Privacy Shield Fee**	**One-time Privacy Shield Arbitral Fund Fee**
$0 to $5 million	$250	$250
Over $5 million to $25 million	$650	$500
Over $25 million to $500 million	$1,000	$1,000
Over $500 million to $5 billion	$2,500	$5,000
Over $5 billion	$3,250	$10,000

2.3. Where to self-certify

Once all requirements have been completed, organisations can self-certify here.

3. KEY CONSIDERATIONS

Organisations that are considering applying for the Privacy Shield should give special consideration to human resources data, sensitive personal data, and law enforcement access requests.

3.1. Human resources data

Organisations that choose to extend the Privacy Shield benefits to human resources personal data transferred from the EU for use in the context of an employment relationship must indicate this when self-certifying. If the self-certification will cover human resources data, then the organisation must agree to use DPAs as an independent resource mechanism with respect to such data (see Section 2.2.3. above). The requirements for onward transfers (see Section 2.2.2. above) also apply to human resources data, but exceptions may be made for occasional employment-related operational needs of the organisation that involve minimal transfers of personal data to third parties (such as booking a flight or hotel room for an employee).

3.2. Sensitive personal data

If the personal data processed by an organisation includes sensitive personal data (data 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), organisations must obtain affirmative express consent from individuals if such information is to be either: disclosed to a third party (see Section 2.2.2. above); or used for a purpose other than as originally collected or as otherwise expressly authorised by the individual.

However, an organisation is not required to obtain affirmative express consent where the processing is:

in the vital interests of the data subject or another person;
necessary for the establishment of legal claims or defenses;
required to provide medical care or diagnosis;
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;
necessary to carry out the organisation's obligations in the field of employment law; or
related to data that are manifestly made public by the individual. In all cases, an organisation should treat as sensitive any personal data received from a third party where the third party identifies and treats it as sensitive.

3.3. Law enforcement access requests

Organisations must inform individuals that personal data may be disclosed in response to lawful requests by public authorities, including for the purposes of meeting national security

or law enforcement requirements. This disclosure is typically included in the organisation's public facing privacy policy.

3.4. Verifying Privacy Shield organisations

Anyone can verify whether an organisation is Privacy Shield certified via the Privacy Shield List. The Privacy Shield List includes, for each certified organisation, the organisational entities covered by the certification, the types of data collected, details about the dispute resolution procedure chosen, and a link to the organisation's privacy policy.

4. ENFORCEMENT

4.1. Supervisory authorities and cooperation procedures

Organisations and their selected independent recourse mechanisms (see Section 2.2.3. above) must respond promptly to inquiries and requests by the Department of Commerce for information relating to an organisation's compliance with the Privacy Shield. Organisations that have chosen DPAs (or, for the Swiss-US Privacy Shield ('the Swiss Privacy Shield'), the Swiss Federal Data Protection and Information Commissioner ('FDPIC') (see Section 5.1.1. below)) must respond directly to such authorities with regard to the investigation and resolution of complaints. While organisations are required to provide all data subjects with the contact information of their chosen independent recourse mechanism provider, the Principles recommend that organisations encourage data subjects to resolve their complaints by first contacting the organisation directly, and then using the independent recourse mechanism if the issue has not been resolved. If no resolution is reached at the level of the independent recourse mechanism provider, complaints can then be brought to arbitration (see Annex I of the Principles).

4.2. Sanctions for non-compliance

The remedies issued by the independent recourse mechanism provider should ensure that any data processing activities of the organisation that are not in compliance with the Principles are brought into compliance. Dispute resolution bodies, including independent recourse mechanism providers and arbitration panels (see Annex I of the Principles), have discretion to implement sanctions corresponding to the severity of the violation. Such sanctions could include publication of findings of non-compliance, the requirement to delete certain personal data, suspension or removal of a seal, financial compensation for data subjects for losses incurred, and injunctions. Dispute resolution bodies must notify the Department of Commerce, and either the FTC or the Department of Transport, as applicable, of an organisation's failure to comply with sanctions.

The FTC may choose to seek an administrative cease-and-desist order or file a complaint in federal court against an organisation that it has reason to believe has violated Section 5 of the FTC Act of 1914 prohibiting unfair or deceptive acts. Such violations may include failure to adhere to the Principles or falsely claiming to be Privacy Shield certified. The FTC has already initiated enforcement actions against several companies for making false claims about their participation in the Privacy Shield.

Where a dispute resolution body has found that an organisation frequently fails to comply with the Principles, the *organisation* must report such findings to the Department of Commerce. Failure by the organisation to do so may be actionable under the False Statements Accountability Act of 1996 (18 USC § 1001). The Department of Commerce will remove organisations from the Privacy Shield List (see Section 3.4. above) in response to persistent failures to comply with the Principles or issued sanctions. Organisations will be provided 30 days' notice and an opportunity to respond before being removed.

5. SWISS-US PRIVACY SHIELD

As with the EU-US Privacy Shield, the Swiss Privacy Shield replaces the old US-Swiss Safe Harbor Framework for organisations transferring personal data from Switzerland to the US. The Principles also apply to the Swiss Privacy Shield, but with a few key distinctions (as outlined below).

5.1. Key distinctions between the Swiss Privacy Shield and the Privacy Shield

Organisations interested in certifying for both the Privacy Shield and the Swiss Privacy Shield should note the following distinctions between the frameworks:

5.1.1. FDPIC

Under the Swiss Privacy Shield, the FDPIC replaces the DPAs as the authoritative regulatory agency. Thus, organisations that process personal data in both Switzerland and EU member states will be subject to the regulatory authority of multiple agencies.

5.1.2. Definition of 'sensitive data'

Under the Swiss Privacy Shield, the definition of 'sensitive data' is slightly broader than under the Privacy Shield, and includes 'ideological views or activities, information on social security measures or administrative or criminal proceedings and sanctions, which are treated outside pending proceedings.'

5.1.3. Binding arbitration option on-hold

While the Swiss Privacy Shield also provides a binding arbitration option as the means for data subjects to resolve residual claims (see Annex I of the Principles), the US International Trade Administration ('ITA') and the FDPIC will not implement this binding arbitration option until the first annual review of the framework, which is scheduled for this year.

5.2. How to certify

Organisations can certify for the Swiss Privacy Shield at the same time as certifying for the Privacy Shield. The link to self-certify can be found here. Organisations that have already self-certified to the Privacy Shield may add the Swiss Privacy Shield to their certification by logging into their existing Privacy Shield account and selecting the Swiss Privacy Shield self-certification option. Those that previously joined the Swiss Safe Harbor will be automatically

withdrawn from the prior framework. Organisations that self-certify for the Swiss Privacy Shield will be required to pay a separate annual fee to the ITA in order to participate, equal to half the amount of the Annual Privacy Shield Fee (see Section 2.2.6. above).

6. PRACTICAL CONSIDERATIONS FOR PREPARING FOR SELF-CERTIFICATION

Organisations must have the Privacy Shield requirements in place before completing the self-certification process and should budget several months for preparation. In practice, the steps for an organisation to undertake, in preparing for self-certification, include:

1. deciding which organisational entities will be included in the self-certification and the types of personal data that will be covered (i.e., HR data or only non-HR data (see Section 3.1 above);
2. updating the organisation's privacy policy;
3. identifying all contracts between the organisation and third party controllers and agents that include transfers of personal data, including both existing signed contracts and contract templates used by the organisation;
4. updating such contracts to include the required Privacy Shield protections (see Section 2.2.2. above) (to the extent the organisation is also in the process of implementing General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR') compliance, it is likely to be most efficient to complete the contract updating process required by GDPR at the same time), which typically involves preparing data processing addendum templates to provide to third parties in relation to existing signed contracts, as well as adding the required language to the organisation's templates (also using a data processing addendum or otherwise);
5. reviewing the organisation's current procedures for providing individuals the ability to exercise their rights to choice and access under the Principles;
6. selecting from the available independent recourse mechanisms and registering with a provider, if applicable;
7. selecting a verification mechanism and registering with a provider, if applicable; and
8. reviewing the organisation's current data security mechanisms to ensure the organisation is providing adequate protection of personal data.

Of the above, the process for updating relevant contracts (i.e., steps 3 – 4 above) is typically the most time-consuming for an organisation, both in terms of identifying all relevant contracts across the organisation and in terms of updating existing signed contracts with third parties (given the potential lack of response or cooperation from the third party, or potential attempts by the third party to negotiate the updated contract). In addition, if the organisation's data security mechanisms are out of date or have not been recently reviewed, the organisation should also expect that this internal review and update process will require significant time and resources to complete.

7. CONCLUDING REMARKS

The Privacy Shield is still a relatively recent framework, and is still subject to further procedural developments and legal challenges. As of 16 February 2018, 2,734 organisations have certified for the Privacy Shield. Many of these organisations are internet-driven

companies, operating in the information and communications technology sector. However, the list also includes business and provisional services providers, healthcare companies, equipment providers, and several others. Any organisation that engages in the importation of personal data from the EEA to the US, and is eligible to self-certify for the Privacy Shield, should consider the scheme as one possible mechanism to satisfy the EU's 'adequate protection' requirement. For organisations that do decide to undergo Privacy Shield self-certification, a thorough review of the requirements and a structured plan, including a timeline, for implementing these requirements, are essential first steps in the process.