Safe Harbor Questionnaire

This questionnaire is aimed at gathering relevant information with regard to the Safe Harbor certification of the data importer. It should be completed by personnel with knowledge of the respective objectives and according to the actual practices within the organization.

The column “Remark/Recommendation” provides guidance/background information for the relevant control objective. In accordance to the control objective, the data importer must state in the column “Actual Practice/Statement/Evidence” its measures, procedures or activities for complying with the control objective. The description of the actual measures can be made in free text form or by referring to supporting documentation. In any case the data importer should provide evidence for the relevant actual practice (through policies, codes of conduct, other documented operational procedures etc.).

#	Control Objective	Remark/Recommendation	Actual Practice/Statement/Evidence
1.	**General Aspects**		
1.1	The self-certification to the Safe Harbor Framework is valid.	*The self-certification to the Safe Harbor Framework has neither expired nor has been revoked by the regulatory body due to noncompliance with its requirements. (http://safeharbor.export.gov/list.aspx)*	
1.2	The organization self-certifies annually to the Department of Commerce in writing that it agrees to adhere to the Safe Harbor’s requirements.	*The organization must designate a Corporate Officer to ensure that the self-certification process is done in a timely manner.*	
1.3	Personal data processed by the organization is covered by the Safe Harbor Framework.	*The Safe Harbor Framework may apply only to certain types of personal data. The organization needs to make sure that personal information received by data exporters from the EU or the EEA are covered by the Safe Harbor Framework.*	
1.4	The organization is subject to the	*The FTC and the DoT can take enforcement*	

	jurisdiction either of the Federal Trade Commission (FTC) or the Department of Transportation (DoT).	*actions against organizations that fail to comply with Safe Harbor. Companies that do not fall under the jurisdiction of either the FTC or DoT would not face a regulatory body with regard to Safe Harbor.*	
1.5	A Corporate Officer is certifying the organization's adherence to the Safe Harbor Framework.	*There must be at least one person in charge making sure the adherence to Safe Harbor.*	
1.6	A designated Organization Contact is handling complaints, access requests, and any other issue under the Safe Harbor Framework.	*Organizations must designate a contact point for handling access requests etc. The contact point can either be the Corporate Officer certifying the company's adherence to Safe Harbor, or other officials within the organization, such as a Chief Privacy Officer.*	
1.7	The organization makes use of verification methods (In-house, Third-Party etc.) verifying the attestations and assertions made about the Safe Harbor privacy practices and its implementation.	*Safe Harbor asks for follow up procedures for verifying the attestations and assertions made about its principles. This can be done by self-assessments or outside compliance reviews (see No. 7, Verification, of the Frequently Asked Questions by the Department of Commerce[1], hereinafter referred to as "FAQ").*	
2.	**Privacy Policy**		
2.1	The organization's privacy policy for personal information has been elaborated and is binding to all business processes.	*The privacy policy statement should reflect the actual and anticipated information handling practices. In addition it has to be clear, concise and easy to understand.* *A sample privacy policy can be found in the International Trade Administration's (ITA) Guide to Self-Certification (http://trade.gov/publications/pdfs/safeharbor-selfcert2009.pdf)*	

[1] http://export.gov/safeharbor/eu/eg_main_018493.asp.

2.2.	The organization's privacy policy for personal information is compliant with the Safe Harbor Principles.	*In order for a privacy policy to be compliant with Safe Harbor, the privacy statement must conform to the seven Privacy Principles and any other relevant points that are covered in the FAQs.*	
2.3	The Policy makes specific reference to the Safe Harbor.	*FAQ No. 6 (Self-Certification) requires all organizations to state in the relevant published privacy policy their adherence to the Safe Harbor.*	
2.4	The Privacy Policy Statement is available to the Public.	*The Privacy Policy Statement has to be made available to the public. A publicly available location is the organization's website for example.*	
2.6	List any privacy programs in which your organization is a member for Safe Harbor Purposes.	*See FAQ No. 6 (Self-Certification) of Safe Harbor. Organizations may qualify for the Safe Harbor in different ways. Organizations can, for example, either join a self-regulatory privacy program that adheres to the Safe Harbor's requirements (e.g. eTrust Safe Harbor program) or develop its own self-regulatory privacy policy that conforms to the Safe Harbor. Please provide in the "Actual Practice/Statement/Evidence" field if your organization developed its own privacy program or joined an existing one.*	
3.	**Contracts**		
	The organization has entered into a written agreement with the data exporter stipulating the obligations for carrying out processing operations.	*Data controllers in the European Union 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, see Safe Harbor FAQ No. 10 (Article 17 Contracts).*	

4.	**Safe Harbor Principles**[2]		
4.1	*Notice*		
a.	Organizations must notify individuals about the purposes for which they collect and use information about them.	*See ITA's guide to self-certification, p. 12.*	
4.2	*Choice*		
a.	Organizations must give data subjects the opportunity to choose (opt out) whether their personal data will be disclosed to a third party or used for a purpose incompatible with the initial purpose.	*See ITA's guide to self-certification, p. 12 ff., et sqq. and FAQ No. 12 (Choice and Timing of Opt-Out).*	
b.	Whether sensitive information is disclosed to a third party or used for a purpose other than its original purpose, individuals must be given an affirmative or explicit choice (opt in).	*See ITA's Self-Certification guide, p. 16 and FAQ No. 1 (Sensitive Data).*	
4.3	*Onwards Transfer*		
a.	In case information is disclosed to a third party the notice and choice principles are applied.	*Please refer to the ITA Self-Certification guide, p. 13.*	
b.	If the organization discloses information to an agent or processor, it has to make sure that the third party subscribes to the Safe Harbor Principles or is subject to the Directive 95/46/EC or any other adequacy finding.	*Please refer to the ITA Self-Certification guide, p. 5 and 13.*	
4.4	*Access*		
a.	The organization makes sure that individuals can access to their personal	*The right of access allows individuals to verify the accuracy of information held about them.*	

[2] Safe Harbor FAQ 10 raises the question, if an organization that adheres to the Safe Harbor needs to comply with all of its Principles when acting merely as data processor for an European data controller. According to European data protection law the Controller remains responsible for the data vis-à-vis the data subject which could lead to the assumption that the Controller should provide for adequate measures with regard to the Principles. On the other hand, US law also applies to questions of interpretation and compliance with the Safe Harbor Principles, which knows no such distinction such as data controller or data processor. Where an US data processor may have no direct contact with European data subjects, the questionnaire should at least indicate how the data processor is cooperating with the original data controller to comply with the Principles.

	data and are able to correct, amend or delete that information where it is inaccurate.	*For additional guidance please refer to the ITA Self-Certification guide, p. 13 and FAQ No. 8 (Access).*	
4.5	*Security*		
a.	The organization takes reasonable precautions to protect personal information from loss, misuse and unauthorized access, disclosure, alteration and destruction.	*The organization has implemented processes and procedures to protect personal information, such as company policies, physical safeguards or other IT-security measures.*	
4.6	*Data integrity*		
	Reasonable steps are made in order to ensure that data is reliable for its intended use, accurate, complete and current.	*Please refer to the ITA Self-Certification guide p. 5 and 13.*	
4.7	*Enforcement*		
	Independent recourse mechanisms are available to investigate unresolved complaints (dispute resolution). As a result of dispute resolution the effects of noncompliance should be reversed or corrected by the organization. Furthermore future processing will be in conformity with the Safe Harbor Principles.	*Please refer to the ITA Self-Certification guide p. 8, Appendix C (List of Dispute Resolution Providers) and FAQ 11 (Dispute Resolution and Enforcement).*	