

Test Location	Process	Activity	CO ID	Control Objective	RP ID	Recommended Practice and Guidance	Actual Practice	Validation Guidance
All Global, Inc. in the European Union (EU) and the European Economic Area (EEA) transferring personal information to the U.S.	Safe Harbor Compliance	Principle of Safe Harbor - Notice	1.1	Data subjects must be informed about the handling of their personal information which is being sent to the United States under the principles of Safe Harbor.	1.1.1	<p>All Global, Inc. in EU and EEA countries must have a process for providing Notice to their data subjects if the data subjects personal data is being transferred to the United States under the Safe Harbor Agreement.</p> <p>The Notice must, at a minimum, include the following details:</p> <ul style="list-style-type: none"> <li>- the purpose for which the data subjects' personal data is collected and used</li> <li>- how to contact the organization with questions/complaints regarding the usage of such personal data</li> <li>- to whom personal data is disclosed</li> </ul> <p>The process for providing notification may vary from country to country. Notice may be provided via:</p> <ul style="list-style-type: none"> <li>- E-mail</li> <li>- Poster</li> <li>- Bulletin Board</li> <li>- Intranet (web announcement)</li> <li>- Post Letter</li> <li>- Other</li> </ul>		
All Global, Inc. in the EU and EEA transferring personal information to the U.S.	Safe Harbor Compliance	Principle of Safe Harbor - Notice	1.1	Notice must be provided prior to the start of collection, processing or disclosure of personal information belonging to EU data subjects.	1.1.2	<p>Notice must be provided when data subjects' personal data is first transferred from EU and EEA countries to the United States under the Safe Harbor Agreement.</p> <p>The Notice must be:</p> <ul style="list-style-type: none"> <li>- appropriately labeled, easy to see, and not in fine print</li> <li>- provided in a timely manner (i.e., prior to the start of the data transfer)</li> <li>- clearly dated to allow data subjects to determine whether the Notice has changed since the last time they read it or since the last time they submitted personal information</li> </ul>		
All Global, Inc. in the EU and EEA transferring personal information to the U.S.	Safe Harbor Compliance	Principle of Safe Harbor - Notice	1.1	Revisions to the Privacy Policies and procedures related to Safe Harbor need to be tracked, documented, and communicated to data subjects.	1.1.3	<p>A record of all revisions made to the Privacy Policy and other procedures related to handling of personal information under the Safe Harbor Agreement must exist. If changes to the policy or the procedures for handling of personal data under the Safe Harbor Agreement are made, then at a minimum, the following information must be documented:</p> <ul style="list-style-type: none"> <li>- the types of changes that were made</li> <li>- the dates those changes were made</li> <li>- the dates those changes were communicated (i.e., date revised policy or procedures were published or distributed; notice was sent)</li> <li>- stored copy of each released version</li> </ul>		
All Global, Inc. in the EU and EEA transferring personal information to the U.S.	Safe Harbor Compliance	Principle of Safe Harbor - Choice	1.2	In the cases when EU data subjects' information needs to be onward transferred from the U.S. to another country, data subjects must be given the option to opt-out of the on-ward transfer or subsequent use of their personal information.	1.2.1	<p>Prior to transferring personal information from the EU and EEA countries under the Safer Harbor Agreement to a third party in the U.S. or to another country, Global, Inc. must ensure that:</p> <ul style="list-style-type: none"> <li>- Notice (fulfilling the requirements set forth by the Notice principle of Safe Harbor) has been provided to data subjects prior to the start of the data transfer (further detail about Notice is available under RP ID 1.1.1 and 2.1.3 in this document)</li> <li>- Data subjects are given an option to opt-out of the onward transfer of their data</li> <li>- If a data subject decides to opt-out of the onward transfer of their data, then Local Global, Inc. along with the Global, Inc. CPO, DPO, or other must assess the reasons for opt-out, address the issues/concerns, and make a final decision on the onward transfer of the data</li> <li>- The decision made by the Local Global, Inc. and the Global, Inc. CPO, DPO, or other, must be in compliance with the Safe Harbor principles and must be communicated to the concerned individual</li> </ul>		

Test Location	Process	Activity	CO ID	Control Objective	RP ID	Recommended Practice and Guidance	Actual Practice	Validation Guidance
All Global, Inc. in the EU and EEA transferring personal information to the U.S.	Safe Harbor Compliance	Principle of Safe Harbor - Choice	1.2	Personal information of EU data subjects is sent to the U.S. only for the purpose defined in the Notice given to data subjects.	1.2.2	<p>A record of all revisions made to the Notice and other procedures related to handling of personal information under the Safe Harbor Agreement must exist.</p> <p>If changes are made to the procedures for handling the personal data under the Safe Harbor Agreement then a new notice must be issued and distributed to data subjects informing them of the changes that were made to the notice which they had previously signed.</p> <p>At a minimum, the following information must be documented:</p> <ul style="list-style-type: none"> <li>- the types of changes that were made to the procedures</li> <li>- the dates those changes were made</li> <li>- the dates those changes were communicated to data subjects (i.e., date revised Notice was distributed)</li> <li>- stored copy of each revised Notice</li> </ul>		
United States	Safe Harbor Compliance	Principle of Safe Harbor - Security	1.3	<p>Organization must take reasonable precautions to protect personal information from loss, misuse, and unauthorized access, disclosure, alteration, and destruction.</p> <p>Processes and procedures are in place to protect access to personal information.</p>	1.3.1	<p>Personal information of EU and EEA data subjects transferred to the U.S. under the Safe Harbor Agreement must be protected from loss, misuse, unauthorized access, disclosure, and destruction.</p> <p>Global, Inc. must have security procedures in place to manage access to such personal information:</p> <ul style="list-style-type: none"> <li>- Access to the personal information must be approved by an appropriate level approver.</li> <li>- Access must be reviewed periodically by an appropriate level reviewer who can assess if a business need for access still exists.</li> <li>- Access must be terminated as soon as a business need for access no longer exists.</li> </ul>		
United States	Safe Harbor Compliance	Principle of Safe Harbor - Security	1.3	<p>Organization must take reasonable precautions to protect personal information from loss, misuse, and unauthorized access, disclosure, alteration, and destruction.</p> <p>Logical controls are in place to protect access to personal information.</p>	1.3.2	<p>Personal information of EU and EEA data subjects transferred to the U.S. under the Safe Harbor Agreement must be protected from loss, misuse, unauthorized access, disclosure, and destruction.</p> <p>(Consider Inserting Company policies and process to be followed by business units)</p>		
United States	Safe Harbor Compliance	Principle of Safe Harbor - Security	1.3	<p>Organization must take reasonable precautions to protect personal information from loss, misuse, and unauthorized access, disclosure, alteration, and destruction.</p> <p>Physical controls are in place to protect access to personal information.</p>	1.3.3	<p>Personal information of EU and EEA data subjects transferred to the U.S. under the Safe Harbor Agreement must be protected from loss, misuse, unauthorized access, disclosure, and destruction.</p> <p>Global, Inc. must utilize physical safeguards as defined by Global, Inc.'s policies and practices to protect such personal information. (Consider Inserting Company policies and process to be followed by business units)</p>		
United States	Safe Harbor Compliance	Principle of Safe Harbor - Integrity	1.4	Controls are in place to protect the integrity of personal information.	1.4.1	<p>Global, Inc. must take reasonable steps to ensure that personal information collected in the EU and EEA countries under the Safe Harbor Agreement is:</p> <ul style="list-style-type: none"> <li>- accurate</li> <li>- complete</li> <li>- current</li> <li>- appropriate for the purposes for which it is collected</li> </ul> <p>Prior to using personal information for the purposes defined in the Notice distributed to data subjects, Global, Inc. must establish a data synchronization process to ensure that personal information stored in U.S. systems matches the personal information stored in European systems.</p>		

Test Location	Process	Activity	CO ID	Control Objective	RP ID	Recommended Practice and Guidance	Actual Practice	Validation Guidance
All Global, Inc. in the EU and EEA transferring personal information to the U.S.	Safe Harbor Compliance	Principle of Safe Harbor - Access	1.5	Data subjects must be given the option to access their personal information and correct it or delete it where inaccurate.	1.5.1	<p>Local Global, Inc. departments in the EU and EEA countries are responsible for maintaining the integrity of personal information by establishing processes that allow data subjects to:</p> <ul style="list-style-type: none"> <li>- access their personal information that is being transferred to the U.S. under the Safe Harbor agreement</li> <li>- request corrections or deletions to their information if inaccurate</li> </ul> <p>Local Global, Inc. departments must ensure that all requests by data subjects for access to or correction of their personal information are properly documented. When corrections to personal information are requested, at a minimum, the following documentation must exist:</p> <ul style="list-style-type: none"> <li>- data of the request</li> <li>- name and contact information of the data subject requesting the change</li> <li>- purpose for the change (i.e., typographical errors, erroneous or outdated data, etc.)</li> <li>- original content</li> <li>- revised content</li> <li>- signature and date</li> <li>- Representative responsible for making the change</li> <li>- change approver</li> <li>- data change was made</li> </ul>		
All Global, Inc. in the EU and EEA transferring personal information to the U.S.	Safe Harbor Compliance	Principle of Safe Harbor - Enforcement	1.6	Process for verifying compliance with Safe Harbor exists.	1.6.1	<p>All EU and EEA countries are required to have a process for monitoring compliance with the Safe Harbor principles. The process should include the following:</p> <ul style="list-style-type: none"> <li>- Each country must complete the Safe Harbor Questionnaire with the actual practices used to ensure compliance with Safe Harbor</li> <li>- Completed questionnaires must be submitted to the Global, Inc.CPO, DPO, or other for review at least annually</li> <li>- Information provided on the actual practices for each country will be used during audits to verify compliance with the Safe Harbor principles</li> </ul>		
United States and all Global, Inc. in the EU and EEA transferring personal information to the U.S.	Safe Harbor Compliance	Principle of Safe Harbor - Enforcement	1.6	Organization must have the ability to resolve complaints as a result of Safe Harbor non-compliance.	1.6.2	<p>Third parties and Global, Inc employees globally must be informed of the corporate policies and procedures regarding the handling of the personal data and the consequences of not complying with those policies and procedures.</p> <p>All data subjects in the EU and EEA countries whose personal information is transferred to the United States under the Safe Harbor Agreement must be informed of the process for filing complaints and disputes regarding the usage of their personal data.</p> <p>The process for handling Safe Harbor related complaints or disputes should include the following steps:</p> <ul style="list-style-type: none"> <li>- Local Global, Inc. receives complaint from data subject</li> <li>- Local Global, Inc. forwards complaint to the Global, Inc.CPO, DPO, or other along with suggestions for resolution</li> <li>- Global, Inc.CPO, DPO, or other reviews complaint and approves recommended resolution</li> <li>- Local Global, Inc. resolves the complaint (along with the Global, Inc.CPO, DPO, or other or his/her delegate, if necessary)</li> <li>- Local Global, Inc. sends a confirmation of resolution back to the Global, Inc.CPO, DPO, or other</li> </ul>		
United States	Safe Harbor Compliance	Principle of Safe Harbor - Onward Transfer	1.7	Prior to sharing personal information with a third party, the entity communicates its privacy policies to and obtains a written agreement from the third party that its practices are substantially equivalent to the entity's.	1.7.1	<p>Prior to transferring personal information from EU and EEA countries under the Safe Harbor Agreement to a third party in the U.S. or to another country, Global, Inc. must ensure that:</p> <ul style="list-style-type: none"> <li>- The third party complies with appropriate personal data handling policies and procedures established by the Global, Inc.CPO, DPO, or other</li> <li>- The Global, Inc.CPO, DPO, or other has granted approval for the transfer of such data to the third party or other country</li> </ul>		

Test Location	Process	Activity	CO ID	Control Objective	RP ID	Recommended Practice and Guidance	Actual Practice	Validation Guidance
United States	Safe Harbor Compliance	Principle of Safe Harbor - Onward Transfer	1.7	Personal information is only disclosed to third parties for the purposes defined in the Notice given to data subjects.	1.7.2	<p>Prior to transferring personal information from the EU and EEA countries under the Safe Harbor Agreement to a third party in the U.S. or to another country, Global, Inc. must ensure that:</p> <ul style="list-style-type: none"> <li>- Notice (fulfilling the requirements set forth by the Notice principle of Safe Harbor) has been provided to data subjects prior to the start of the data transfer (further detail about Notice is available under RP ID 1.1.1, 1.1.2, and 2.1.3 in this document)</li> <li>- Any changes to the purpose for which personal information is being transferred/disclosed to third parties are documented in a new Notice which is provided to data subjects prior to the start of the transfer</li> </ul>		
United States	Safe Harbor Compliance	Principle of Safe Harbor - Enforcement	2.1	A Safe Harbor recertification must be signed by a corporate officer or authorized representative once a year.	2.1.1	<p>Global Inc.'s Safe Harbor recertification is filed with the U.S. Department of Commerce (<a href="http://www.export.gov/safeharbor">http://www.export.gov/safeharbor</a>) annually on January 1, 20XX. The U.S. Department of Commerce website contains the most updated list of all certified companies. The Certification is signed by the Officer or other authorized individual of Global, Inc.</p>		
United States and all Global, Inc. in the EU and EEA transferring personal information to the U.S.	Safe Harbor Compliance	Principle of Safe Harbor - Enforcement	2.1	Compliance with Safe Harbor is reviewed annually through a self-assessment and/or an independent compliance review.	2.1.2	<p>Objective verifiable audits of compliance with the Safe Harbor Framework will be performed by Global Inc.'s Audit Services or other third party audit service for selected countries every year. In addition, all business units globally will participate in an annual Self-assessment. Results of the audits as well as any self-assessments completed by EU and EEA countries must be submitted to the Global CPO, DPO, or other annually. The due dates for self-assessments will be communicated to Local Global, Inc. by the Global, Inc. CPO, DPO, or other on an annual basis.</p>		
United States and all Global, Inc. in the EU and EEA transferring personal information to the U.S.	Safe Harbor Compliance	Principle of Safe Harbor - Enforcement	2.1	Privacy Policy addresses the Safe Harbor Principle of Notice.	2.1.3	<p>A privacy policy addressing the Notice principle of Safe Harbor exists.</p> <p>Notice - Organizations must notify data subjects about the purposes for which they collect and use information about them. They must provide information about how data subjects can contact the organization with any inquiries or complaints, the types of third parties to which it discloses the information and the choices and means the organization offers for limiting its use and disclosure.</p>		

Test Location	Process	Activity	CO ID	Control Objective	RP ID	Recommended Practice and Guidance	Actual Practice	Validation Guidance
United States and all Global, Inc. in the EU and EEA transferring personal information to the U.S.	Safe Harbor Compliance	Principle of Safe Harbor - Enforcement	2.1	Privacy Policy addresses the Safe Harbor Principle of Choice.	2.1.4	<p>A privacy policy addressing the Choice principle of Safe Harbor exists.</p> <p>Choice - Organizations must give data subjects the opportunity to choose (opt out) whether their personal information will be disclosed to a third party or used for a purpose incompatible with the purpose for which it was originally collected or subsequently authorized by the individual. For sensitive information, affirmative or explicit (opt in) choice must be given if the information is to be disclosed to a third party or used for a purpose other than its original purpose or the purpose authorized subsequently by the individual.</p>		
United States and all Global, Inc. in the EU and EEA transferring personal information to the U.S.	Safe Harbor Compliance	Principle of Safe Harbor - Enforcement	2.1	Privacy Policy addresses the Safe Harbor Principle of Onward Transfer.	2.1.5	<p>A privacy policy addressing the Onward Transfer principle of Safe Harbor exists.</p> <p>Onward Transfer (Transfer to Third Parties) - To disclose information to a third party, organizations must apply the notice and choice principles. Where an organization wishes to transfer information to a third party that is acting as an agent(1), it may do so if it makes sure that the third party subscribes to the safe harbor principles or is subject to the Directive or another adequacy finding. As an alternative, the organization can enter into a written agreement with such third party requiring that the third party provide at least the same level of privacy protection as is required by the relevant principles.</p>		
United States and all Global, Inc. in the EU and EEA transferring personal information to the U.S.	Safe Harbor Compliance	Principle of Safe Harbor - Enforcement	2.1	Privacy Policy addresses the Safe Harbor Principle of Access.	2.1.6	<p>A privacy policy addressing the Access principle of Safe Harbor exists.</p> <p>Access - data subjects 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, 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.</p>		
United States and all Global, Inc. in the EU and EEA transferring personal information to the U.S.	Safe Harbor Compliance	Principle of Safe Harbor - Enforcement	2.1	Privacy Policy addresses the Safe Harbor Principle of Security.	2.1.7	<p>A privacy policy addressing the Security principle of Safe Harbor exists.</p> <p>Security - Organizations must take reasonable precautions to protect personal information from loss, misuse and unauthorized access, disclosure, alteration and destruction.</p>		
United States and all Global, Inc. in the EU and EEA transferring personal information to the U.S.	Safe Harbor Compliance	Principle of Safe Harbor - Enforcement	2.1	Privacy Policy addresses the Safe Harbor Principle of Data Integrity.	2.1.8	<p>A privacy policy addressing the Data Integrity principle of Safe Harbor exists.</p> <p>Data Integrity - personal information must be relevant for the purposes for which it is to be used. An organization should take reasonable steps to ensure that data is reliable for its intended use, accurate, complete, and current.</p>		
United States and all Global, Inc. in the EU and EEA transferring personal information to the U.S.	Safe Harbor Compliance	Principle of Safe Harbor - Enforcement	2.1	Privacy Policy addresses the Safe Harbor Principle of Enforcement.	2.1.9	<p>A privacy policy addressing the Enforcement principle of Safe Harbor exists.</p> <p>Enforcement - In order to ensure compliance with the Safe Harbor principles, there must be (a) readily available and affordable independent recourse mechanisms so that each individual's complaints and disputes can be investigated and resolved and damages awarded where the applicable law or private sector initiatives so provide; (b) procedures for verifying that the commitments companies make to adhere to the safe harbor principles have been implemented; and (c) obligations to remedy problems arising out of a failure to comply with the principles. Sanctions must be sufficiently rigorous to ensure compliance by the organization. Organizations that fail to provide annual self certification letters will no longer appear in the list of participants and safe harbor benefits will no longer be assured.</p>		

Test Location	Process	Activity	CO ID	Control Objective	RP ID	Recommended Practice and Guidance	Actual Practice	Validation Guidance
United States and all Global, Inc. in the EU and EEA transferring personal information to the U.S.	Safe Harbor Compliance	Principle of Safe Harbor - Enforcement	2.1	Employees who work with personal information are trained on cross-border data transfers and proper data handling procedures under the Safe Harbor Agreement.	2.1.10	<p>All personnel who handle personal information of data subjects from EU and EEA countries covered under the Safe Harbor Agreement must be trained on the appropriate methods of handling such data.</p> <p>Global, Inc. must developed training materials detailing appropriate procedures for handling personal information and cross-border data transfers. Completing a training session is mandatory for all such personnel handling the personal information transferred and a process to track compliance with these training requirements must be developed. Documentation detailing at least the following must be maintained for all personnel involved with personal information handling and cross-border data transfers:</p> <ul style="list-style-type: none"> <li>- Name, title, location, and contact information</li> <li>- Training type, training topic, and date of training completion</li> </ul>		