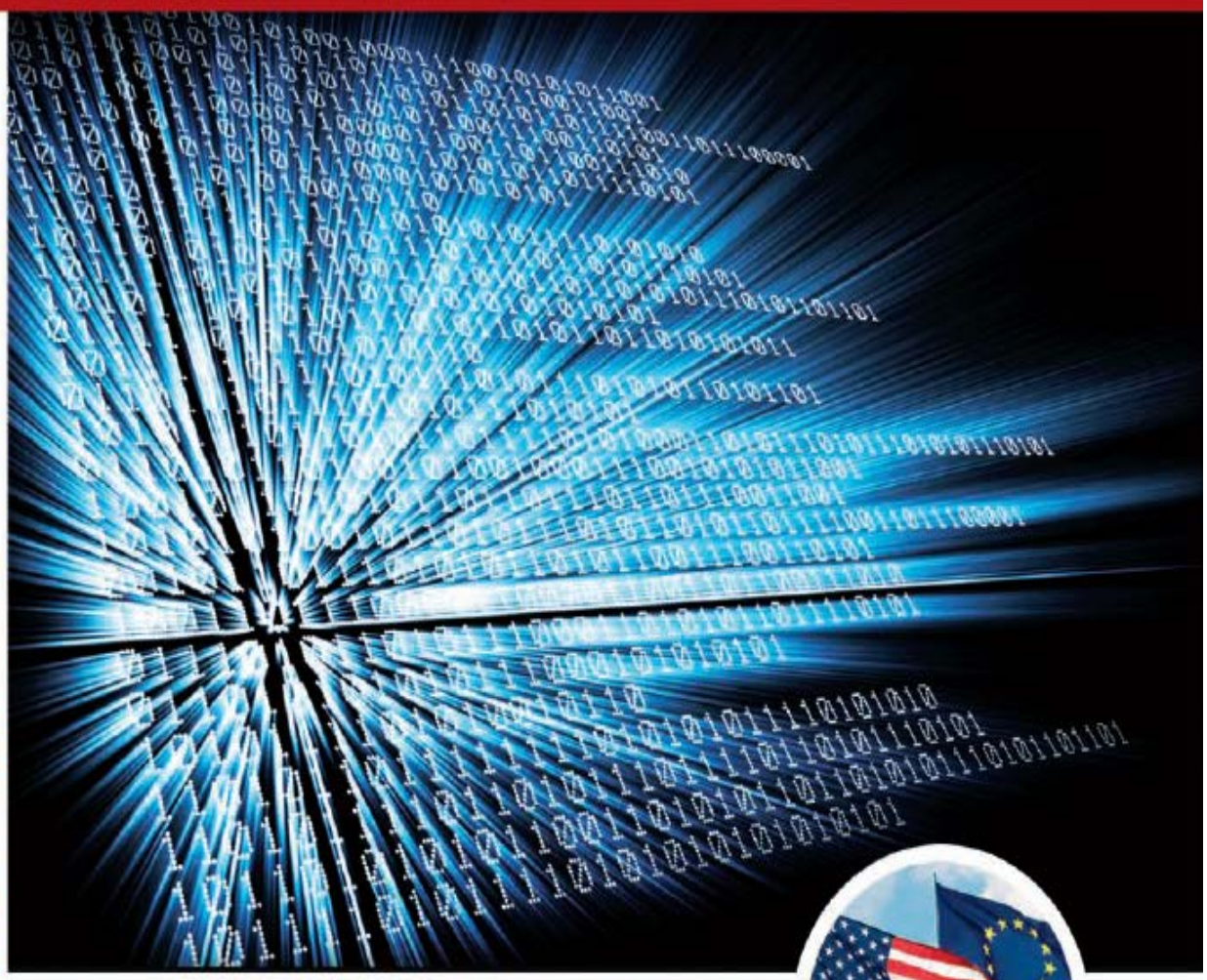
U.S. ★ EU SAFE HARBOR FRAMEWORK ★ GUIDE TO SELF-CERTIFICATION



GUIDE TO SELF-CERTIFICATION

U.S. ★ EU SAFE HARBOR FRAMEWORK

U.S.-EU Safe Harbor Framework

A Guide to Self-Certification

Table of Contents

Introduction

Welcome to the U.S.-European Union (EU) Safe Harbor Framework: A Guide to Certification. It is our hope that the Guide will provide U.S. organizations with a better understanding of the purpose and process of self-certifying compliance with the U.S.-EU Safe Harbor Framework. Additional information is available on our website: http://export.gov/safeharbor/

In this Guide, we have outlined the critical components of the U.S.-EU Safe Harbor Framework. We have included not only Helpful Hints on Self-Certifying Compliance, but also a copy of the certification form. The Safe Harbor Privacy Principles and frequently asked questions (FAQs) have also been provided for easy reference. In addition, we have included several examples of organization privacy policies. Finally, we have provided a list of third-party dispute resolution providers and a glossary of key terms. The Guide is divided into nine major sections. What follows is a brief description of each section:

Overview: The Overview provides background on the U.S.-EU Safe Harbor Framework, including how it came about, the benefits of participation, and the basic eligibility criteria. The Overview also provides a summary of what the Safe Harbor Privacy Principles require.

Helpful Hints on Self-Certifying Compliance: The Helpful Hints are meant to provide quick answers to any questions U.S. organizations might have about the self-certification process, but this resource should be used in conjunction. It should be used in conjunction with the rest of the Guide. The Helpful Hints also serve as a checklist, which should be reviewed to evaluate an organization's readiness to self-certify.

Safe Harbor Privacy Principles: We have provided the full text of the official declaration of the Safe Harbor Privacy Principles, as announced on July 21, 2000. This text is helpful in understanding the foundation of the Safe Harbor Privacy Principles and the U.S.-EU Safe Harbor Framework.

Frequently Asked Questions (FAQs): The FAQs and answers, which clarify and supplement the Safe Harbor Privacy Principles, address many of the most commonly asked questions about the U.S.-EU Safe Harbor Framework.

Certification Form: We have provided the Certification Form for easy reference, as it serves as the self-certification application form. Once submitted and approved, a completed certification form serves as a participating organization's Safe Harbor List record. Applicants should apply online via our website (i.e. click on the "Safe Harbor Login / Certification Form" link on the left navigation bar: https://safeharbor.export.gov/login.aspx).

Sample Privacy Policies: We have provided three sample privacy policies, which may serve as guidance when creating a new privacy policy or updating an existing one to conform to the U.S.-EU Safe Harbor Framework. Relevant privacy policies must include an affirmative commitment to the Safe Harbor Privacy Principles and the U.S.-EU Safe Harbor Framework.

Dispute Resolution Options: We have provided a short description of the role of third-party dispute resolution providers (also referred to as 'independent recourse mechanisms'), a list of such providers, and descriptions of the services provided by three of the listed providers.

Certification Mark: The U.S. Department of Commerce's International Trade Administration (ITA) developed a certification mark for the U.S.-EU Safe Harbor Framework, which may be used by participating organizations on their websites to signify that they have self-certified compliance with the provisions of the U.S.-EU Safe Harbor Framework. We have provided the instructions on the proper use of the certification mark.

Glossary: A short glossary is also provided for many of the technical terms frequently used in the Guide.

Safe Harbor Overview

Background on the U.S.-EU Safe Harbor

When the European Commission's Directive on Data Protection went into effect in October of 1998, one consequence was to prohibit the transfer of personal data to non-European Union countries that do not meet the European Union (EU) "adequacy" standard for privacy protection. While the United States and the EU share the goal of enhancing privacy protection for their citizens, the United States takes a different approach to privacy from that taken by the EU. The United States uses a sectoral approach that relies on a mix of legislation, regulation, and self-regulation. The EU, however, relies on comprehensive legislation that requires, among other things, the creation of independent government data protection agencies, registration of databases with those agencies, and in some instances prior approval before data processing may begin. As a result of these differences, the Directive could have significantly hampered the ability of U.S. organizations to engage in a range of trans-Atlantic transactions.

In order to bridge these differences in approach and provide a streamlined and cost-effective means for U.S. organizations to satisfy the Directive's "adequacy" requirement, the U.S. Department of Commerce in consultation with the European Commission (EC) developed a "Safe Harbor" framework and a website to provide the information an organization would need to evaluate – and then join – the Safe Harbor.

The U.S.-EU Safe Harbor Framework, which was approved by the EU in 2000, is an important way for U.S. organizations to avoid experiencing interruptions in their business dealings with the EU or facing prosecution by EU member state authorities under EU member state privacy laws. Self-certifying to the U.S.-EU Safe Harbor Framework will ensure that EU organizations know that your organization provides "adequate" privacy protection, as defined by the Directive.

Safe Harbor Benefits

The U.S.-EU Safe Harbor Framework provides a number of important benefits to U.S. and EU organizations.

Benefits for U.S. organizations participating in the Safe Harbor include:

- All 27 Member States of the European Union will be bound by the European Commission's finding of adequacy;
- Organizations participating in the U.S.-EU Safe Harbor program will be deemed to provide "adequate" privacy protection;
- Member State requirements for prior approval of data transfers either will be waived or approval will be automatically granted;
- Claims brought by European citizens against U.S. organizations will be heard, subject to limited exceptions, in the United States; and
- Compliance requirements are streamlined and cost-effective, which should particularly benefit small and medium enterprises.

An EU organization can ensure that it is sending information to a U.S. organization participating in the U.S.-EU Safe Harbor program by viewing the public list of Safe Harbor organizations posted on the Safe Harbor website. This list contains the names of all U.S. organizations that have self-certified to the U.S.-EU Safe Harbor Framework. This list will be updated regularly, so that it is clear which organizations are assured of Safe Harbor benefits.

How does an organization join?

The decision by U.S. organizations to enter the U.S.-EU Safe Harbor program is entirely voluntary. Organizations that decide to participate in the U.S.-EU Safe Harbor program must comply with the U.S.-EU Safe Harbor Framework and publicly declare that they do so. To be assured of Safe Harbor benefits, an organization must to self-certify annually in writing to the Department of Commerce that it agrees to adhere to the U.S.-EU Safe Harbor program's requirements, which include elements such as notice, choice, access, and enforcement. It must also state in its published privacy policy statement that it complies with the U.S.-EU Safe Harbor Framework and that it has certified its adherence to the Safe Harbor Privacy Principles. The Department of Commerce maintains a list of the organizations that file self-certification letters and makes both the list and the self-certification letters publicly available.

To qualify for the U.S.-EU Safe Harbor, an organization can either join a self-regulatory privacy program that adheres to the Safe Harbor's requirements or develop its own self-regulatory privacy policy that conforms to the Safe Harbor. Moreover, only those organizations subject to the jurisdiction of the Federal Trade Commission (FTC) or U.S. air carriers and ticket agents subject to the jurisdiction of the Department of Transportation (DoT) may participate in the Safe Harbor. Organizations generally not subject to FTC jurisdiction include certain financial institutions (e.g. banks, investment houses, credit unions, and savings & loans institutions), telecommunication common carriers, labor organizations, non-profit organizations, agricultural cooperatives, and meat-processing facilities. If you are uncertain as to whether your organization falls under the jurisdiction of either the FTC or DoT, as certain exceptions to general ineligibility do exist, be sure to contact those agencies for more information.

What do the Safe Harbor principles require?

Organizations must comply with the seven Safe Harbor Privacy Principles, which require the following:

1. Notice

Organizations must notify individuals about the purposes for which they collect and use information about them. They must provide information about how individuals can contact the organization with any inquiries or complaints, the types of third parties to which they disclose the information and the choices and means the organization offers for limiting its use and disclosure.

2. Choice

Organizations must give individuals 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.

3. Onward Transfer (Transfers 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, it may do so if it makes sure that the third party subscribes to the Safe Harbor Privacy 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.

4. Access

Individuals must have access to personal information about themselves 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.

5. Security

Organizations must take reasonable precautions to protect personal information from loss, misuse and unauthorized access, disclosure, alteration and destruction.

6. 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.

7. Enforcement

In order to ensure compliance with the Safe Harbor Privacy 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 Privacy Principles have been implemented; and (c) obligations to remedy problems arising out of a failure to comply with the Safe Harbor Privacy Principles. Sanctions must be sufficiently rigorous to ensure compliance by the organization. Organizations that fail to provide annual self-certification letters reaffirming their commitment to the U.S.-EU Safe Harbor Framework and/or the U.S.-Swiss Safe Harbor Framework will no longer be assured of the relevant Safe Harbor benefits and may ultimately be removed from the list of participants maintained on the Safe Harbor website.

The Department of Commerce has issued a set of frequently asked questions and answers (FAQs) that clarify and supplement the Safe Harbor Privacy Principles.

Helpful Hints on Self-Certifying Compliance

This section contains helpful hints on self-certifying compliance with the U.S.-EU Safe Harbor Framework and serves as a checklist that should be reviewed to evaluate an organization's readiness to self-certify. Although this section provides succinct answers to many of common questions regarding the self-certification process, this resource should be used in conjunction with the rest of the Guide, including the requirements for self-certification detailed in FAQ 6.

The topics covered below include: determining whether your organization is subject to the jurisdiction of an appropriate statutory authority, developing a Safe Harbor compliant privacy policy statement, establishing a suitable independent recourse mechanism, ensuring that a suitable verification method is in place, and designating a contact within your organization regarding Safe Harbor.

Confirm that Your Organization is Subject to the Jurisdiction of the U.S. Federal Trade Commission or the U.S. Department of Transportation: Any U.S. organization that is subject to the jurisdiction of the Federal Trade Commission (FTC) or U.S. air carriers and ticket agents subject to the jurisdiction of the Department of Transportation (DoT) may participate in the Safe Harbor. The FTC and DoT have both stated in letters to the European Commission (located with the Framework Document under Letters G and H) that they will take enforcement action against organizations that state that they are in compliance with the Framework, but then fail to live up to their statements. If you are uncertain as to whether your organization falls under the jurisdiction of either the FTC or DoT, the please be sure to contact those agencies for more information.

Develop a Safe Harbor Compliant Privacy Policy Statement:

Remember to develop a Safe Harbor compliant privacy policy statement before submitting a self-certification form to the Department of Commerce.

- **Make Sure That Your Privacy Policy Statement Conforms to the U.S.-EU Safe Harbor Privacy Principles:** In order for a privacy policy to be compliant with the Framework, the privacy policy must conform to the seven Safe Harbor Privacy Principles, as well as any relevant points covered in the Frequently Asked Questions (FAQs), which are located with the other Framework documents. In addition, the privacy policy should reflect your organization's actual and anticipated information handling practices. It is also important to write a policy that is clear, concise, and easy to understand.

- **Make Specific Reference in the Text of Your Privacy Policy to Your Organization's Safe Harbor Compliance:** FAQ 6 requires each organization that self-certifies to state in its applicable published privacy policy that it complies with the U.S.-EU Safe Harbor Framework and that it has certified its adherence to the Safe Harbor Privacy Principles. In addition, each organization should include either a hyperlink to the Safe Harbor website or the corresponding URL (e.g., http://export.gov/safeharbor).
- **Provide an Accurate Privacy Policy Location and Make Sure that Your Privacy Policy is Available to the Public:** At the time of self-certification, each organization must provide an accurate location for its applicable privacy policy. In addition, each organization should verify that its privacy policy is effective prior to self-certification. If your organization decides to post your privacy policy on an Internet or Intranet site, it must provide an accurate URL.
    - If your organization: 1) has a public website on which it has posted a general privacy policy statement or made any other representation regarding its privacy practices; and 2) has chosen to cover personal data (e.g., client or customer data) other than your organization's own human resources data under its self-certification, then the posted privacy-related language must include an affirmative statement that your organization complies with the U.S.-EU Safe Harbor Framework and has certified its adherence to the Safe Harbor Privacy Principles (i.e., it is not sufficient to simply upload a privacy policy to your organization's Safe Harbor submission). In addition, the posted privacy-related language must also include either a hyperlink to the Safe Harbor website or the corresponding URL (e.g., http://export.gov/safeharbor/).
    - If the information covered by your organization's self-certification exclusively relates to your own organization's human resources data, then the privacy policy covering such data need only be made available to your organization's employees and as part of the Safe Harbor review process (i.e., your organization is not required to upload a copy to your organization's Safe Harbor submission, but it is encouraged do so). If such a policy is listed as being located at corporate headquarters or on the corporate Intranet or is otherwise inaccessible to the general public via your organization's public website, then your organization must provide the Department of Commerce with a copy of the policy so that it can be reviewed. If a copy of such a policy is provided for the reason just described, your organization must clarify whether or not it would object to having the copy uploaded to your organization's Safe Harbor submission.

Establish Your Organization's Independent Recourse Mechanism: Under the Framework's Enforcement Principle, organizations self-certifying must establish an independent recourse mechanism available to investigate unresolved complaints. (See FAQ 11 for more information regarding dispute resolution under Safe Harbor.) The organization must ensure that its recourse mechanism is in place prior to self-certification. In addition, each organization should include in its privacy policy an appropriate reference to the independent recourse mechanism(s), as well as relevant contact information for said mechanism(s).

In most cases, organizations self-certifying to Safe Harbor may choose to utilize private sector dispute resolution programs. While programs vary, organizations like BBB EU Safe Harbor Program, TRUSTe, the Direct Marketing Association, the Entertainment Software Rating Board, JAMS and the American Arbitration Association have developed programs that assist in compliance with the Framework's Enforcement Principle and FAQ 11.

Alternatively, organizations may choose to cooperate and comply with the EU Data Protection Authorities (DPAs) with respect to all types of data. In doing so, an organization must follow the procedures outlined in FAQ 5. If **organization human resources data** (i.e. personal information about your organization's own employees, past or present, collected in the context of the employment relationship) is being covered in your organization's self-certification, your organization must agree to cooperate and comply with the EU DPAs with respect to such data. Additional guidance on the handling of human resources data under the Framework is provided in FAQ 9.

- Organizations that either choose to or must utilize the EU DPAs are required to pay an **annual fee of US $50** in order to cover the operating costs of the panel established by the EU DPAs to resolve disputes pursuant to the Safe Harbor Privacy Principles. This fee is payable to the United States Council for International Business (U.S. Council for International Business c/o Safe Harbor – EU DPAs; 1212 Avenue of the Americas, 21st Floor; New York, NY 10036), which has agreed to act as trusted third party for this purpose. If your organization requires further information on how to carry out the payment, please see: http://uscib.org/index.asp?documentID=4495.
- If your organization requires further information on how the cooperation / compliance with the EU DPAs works, your organization may refer to the resources concerning the EU DPA panel (e.g., the Standard Complaint Form and Internal Operating Procedures) that are available on the European Commission's website (see http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/), contact the EU DPA panel secretariat at: ec-dppanel-secr@ec.europa.eu, and/or contact the DPAs directly (see http://ec.europa.eu/justice/data-protection/bodies/authorities/eu/index_en.htm).

Ensure That Your Organization's Verification Mechanism is in Place: As discussed in FAQ 7, organizations self-certifying to the Framework are required to have procedures in place for verifying compliance. To meet this requirement, an organization may use either a self-assessment or an outside/third-party assessment program. For additional guidance on the Safe Harbor's verification requirement, please see FAQ 7.

Designate a Contact within Your Organization Regarding Safe Harbor: Each organization is required to provide a contact for the handling of questions, complaints, access requests, and any other issues arising under the Safe Harbor. This contact can be either the corporate officer that is certifying your organization's adherence to Safe Harbor, or another official within the organization, such as a Chief Privacy Officer.

Safe Harbor Privacy Principles

U.S.-EU Safe Harbor Privacy Principles

Issued by the U.S. Department of Commerce on July 21, 2000

The European Union's comprehensive privacy legislation, the Directive on Data Protection (the Directive), became effective on October 25, 1998. It requires that transfers of personal data take place only to non-EU countries that provide an "adequate" level of privacy protection. While the United States and the European Union share the goal of enhancing privacy protection for their citizens, the United States takes a different approach to privacy from that taken by the European Union. The United States uses a sectoral approach that relies on a mix of legislation, regulation, and self-regulation. Given those differences, many U.S. organizations have expressed uncertainty about the impact of the EU-required "adequacy standard" on personal data transfers from the European Union to the United States.

To diminish this uncertainty and provide a more predictable framework for such data transfers, the Department of Commerce is issuing this document and Frequently Asked Questions ("the Principles") under its statutory authority to foster, promote, and develop international commerce. The Principles were developed in consultation with industry and the general public to facilitate trade and commerce between the United States and European Union. They are intended for use solely by U.S. organizations receiving personal data from the European Union for the purpose of qualifying for the Safe Harbor and the presumption of "adequacy" it creates. Because the Principles were solely designed to serve this specific purpose, their adoption for other purposes may be inappropriate. The Principles cannot be used as a substitute for national provisions implementing the Directive that apply to the processing of personal data in the Member States.

Decisions by organizations to qualify for the Safe Harbor are entirely voluntary, and organizations may qualify for the Safe Harbor in different ways. Organizations that decide to adhere to the Principles must comply with the Principles in order to obtain and retain the benefits of the Safe Harbor and publicly declare that they do so. For example, if an organization joins a self-regulatory privacy program that adheres to the Principles, it qualifies for the Safe Harbor. Organizations may also qualify by developing their own self-regulatory privacy policies provided that they conform with the Principles. Where in complying with the Principles, an organization relies in whole or in part on self-regulation, its failure to

comply with such self-regulation must also be actionable under Section 5 of the Federal Trade Commission Act prohibiting unfair and deceptive acts or another law or regulation prohibiting such acts. *(See the annex for the list of U.S. statutory bodies recognized by the EU.)* In addition, organizations subject to a statutory, regulatory, administrative or other body of law (or of rules) that effectively protects personal privacy may also qualify for Safe Harbor benefits. In all instances, Safe Harbor benefits are assured from the date on which each organization wishing to qualify for the Safe Harbor self-certifies to the Department of Commerce (or its designee) its adherence to the Principles in accordance with the guidance set forth in the Frequently Asked Question on Self-Certification**.**

Adherence to these Principles may be limited: (a) to the extent necessary to meet national security, public interest, or law enforcement requirements; (b) by statute, government regulation, or case law that create conflicting obligations or explicit authorizations, provided that, in exercising any such authorization, an organization can demonstrate that its non-compliance with the Principles is limited to the extent necessary to meet the overriding legitimate interests furthered by such authorization; or (c) if the effect of the Directive or Member State law is to allow exceptions or derogations, provided such exceptions or derogations are applied in comparable contexts. Consistent with the goal of enhancing privacy protection, organizations should strive to implement these Principles fully and transparently, including indicating in their privacy policies where exceptions to the Principles permitted by (b) above will apply on a regular basis. For the same reason, where the option is allowable under the Principles and/or U.S. law, organizations are expected to opt for the higher protection where possible.

Organizations may wish for practical or other reasons to apply the Principles to all their data processing operations, but they are only obligated to apply them to data transferred after they enter the Safe Harbor. To qualify for the Safe Harbor, organizations are not obligated to apply these Principles to personal information in manually processed filing systems. Organizations wishing to benefit from the Safe Harbor for receiving information in manually processed filing systems from the EU must apply the Principles to any such information transferred after they enter the Safe Harbor. An organization that wishes to extend Safe Harbor benefits to human resources personal information transferred from the EU for use in the context of an employment relationship must indicate this when it self-certifies to the Department of Commerce (or its designee) and conform to the requirements set forth in the Frequently Asked Question on Self-Certification.

Organizations will also be able to provide the safeguards necessary under Article 26 of the Directive if they include the Principles in written agreements with parties transferring data from the EU for the substantive privacy provisions, once the other provisions for such model contracts are authorized by the Commission and the Member States.

U.S. law will apply to questions of interpretation and compliance with the Safe Harbor Principles (including the Frequently Asked Questions) and relevant privacy policies by Safe Harbor organizations, except where organizations have committed to cooperate with European Data Protection Authorities. Unless otherwise stated, all provisions of the Safe Harbor Principles and Frequently Asked Questions apply where they are relevant.

"Personal data" and "personal information" are data about an identified or identifiable individual that are within the scope of the Directive, received by a U.S. organization from the European Union, and recorded in any form.

Notice: An organization must inform individuals about the purposes for which it collects and uses information about them, how to 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 individuals for limiting its use and disclosure. This notice must be provided in clear and conspicuous language when individuals are first asked to provide personal information to the organization or as soon thereafter as is practicable, but in any event before the organization uses such information for a purpose other than that for which it was originally collected or processed by the transferring organization or discloses it for the first time to a third party(1).

Choice: An organization must offer individuals the opportunity to choose (opt out) whether their personal information is (a) to be disclosed to a third party(1) or (b) to be used for a purpose that is incompatible with the purpose(s) for which it was originally collected or subsequently authorized by the individual. Individuals must be provided with clear and conspicuous, readily available, and affordable mechanisms to exercise choice.

For sensitive information (i.e. personal information 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), they must be given affirmative or explicit (opt in) choice if the information is to be disclosed to a third party or used for a purpose other than those for which it was originally collected or subsequently authorized by the individual through the exercise of opt in choice.

In any case, an organization should treat as sensitive any information received from a third party where the third party treats and identifies it as sensitive.

Onward Transfer: 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, as described in the endnote, it may do so if it first either ascertains that the third party subscribes to the Principles or is subject to the Directive or another adequacy finding or enters 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. If the organization complies with these requirements, it shall not be held responsible (unless the organization agrees otherwise) when a third party to which it transfers such information processes it in a way contrary to any restrictions or representations, unless the organization knew or should have known the third party would process it in such a contrary way and the organization has not taken reasonable steps to prevent or stop such processing.

Security: Organizations creating, maintaining, using or disseminating personal information must take reasonable precautions to protect it from loss, misuse and unauthorized access, disclosure, alteration and destruction.

Data Integrity: Consistent with the Principles, personal information must be relevant for the purposes for which it is to be used. An organization may not process personal information in a way that is incompatible with the purposes for which it has been collected or subsequently authorized by the individual. To the extent necessary for those purposes, an organization should take reasonable steps to ensure that data is reliable for its intended use, accurate, complete, and current.

Access: Individuals 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.

Enforcement: Effective privacy protection must include mechanisms for assuring compliance with the Principles, recourse for individuals to whom the data relate affected by non-compliance with the Principles, and consequences for the organization when the Principles are not followed. At a minimum, such mechanisms must include (a) readily available and affordable independent recourse mechanisms by which each individual's complaints and disputes are investigated and resolved by reference to the Principles and damages awarded where the applicable law or private sector initiatives so provide; (b) follow up procedures for verifying that the attestations and assertions businesses make about their privacy practices are true and that privacy practices have been implemented as presented; and (c) obligations to remedy problems arising out of failure to comply with the Principles by organizations announcing their adherence to them and consequences for such organizations. Sanctions must be sufficiently rigorous to ensure compliance by organizations.

1. It is not necessary to provide notice or choice when disclosure is made to a third party that is acting as an agent to perform task(s) on behalf of and under the instructions of the organization. The Onward Transfer Principle, on the other hand, does apply to such disclosures.

Frequently Asked Questions (FAQs)

This section contains frequently asked questions (FAQs) regarding the U.S.-EU Safe Harbor Framework. Divided into fifteen (15) sections, these represent the most commonly asked questions covering the rights of data subjects; obligations and interactions between data subjects, handlers and third parties; and topics including the certification process, liabilities and enforcement, sector-specific rules and exceptions, and potential "what ifs" in the Safe Harbor context.

U.S.-EU Safe Harbor Framework Frequently Asked Questions (FAQs)

I. Sensitive Data

Q: Must an organization always provide explicit (opt in) choice with respect to sensitive data?

A: No, such choice is not required where the processing is: (1) in the vital interests of the data subject or another person; (2) necessary for the establishment of legal claims or defenses; (3) required to provide medical care or diagnosis; (4) 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; (5) necessary to carry out the organization's obligations in the field of employment law; or (6) related to data that are manifestly made public by the individual.

II. Journalistic Exceptions

Q: Given U.S. constitutional protections for freedom of the press and the Directive's exemption for journalistic material, do the Safe Harbor Principles apply to personal information gathered, maintained, or disseminated for journalistic purposes?

A: Where the rights of a free press embodied in the First Amendment of the U. S. Constitution intersect with privacy protection interests, the First Amendment must govern the balancing of these interests with regard to the activities of U.S. persons or organizations. Personal information that is gathered for publication, broadcast, or other forms of public communication of journalistic material, whether used or not, as well as information found in previously published material disseminated from media archives, is not subject to the requirements of the Safe Harbor Principles.

III. Secondary Liability

Q: Are Internet service providers (ISPs), telecommunications carriers, or other organizations liable under the Safe Harbor Principles when on behalf of another organization they merely transmit, route, switch or cache information that may violate their terms?

A: No. As is the case with the Directive itself, the Safe Harbor does not create secondary liability. To the extent that an organization is acting as a mere conduit for data transmitted by third parties and does not determine the purposes and means of processing those personal data, it would not be liable.

IV. Investment banking and audits

Q: The activities of auditors and investment bankers may involve processing personal data without the consent or knowledge of the individual. Under what circumstances is this permitted by the Notice, Choice, and Access Principles?

A: Investment bankers or auditors may process information without knowledge of the individual only to the extent and for the period necessary to meet statutory or public interest requirements and in other circumstances in which the application of these Principles would prejudice the legitimate interests of the organization. These legitimate interests include the monitoring of companies' compliance with their legal obligations and legitimate accounting activities, and the need for confidentiality connected with possible acquisitions, mergers, joint ventures, or other similar transactions carried out by investment bankers or auditors.

V. The Role of the Data Protection Authorities

Q: How will companies that commit to cooperate with European Union Data Protection Authorities (DPAs) make those commitments and how will they be implemented?

A: Under the Safe Harbor, U.S. organizations receiving personal data from the EU must commit to employ effective mechanisms for assuring compliance with the Safe Harbor Principles. More specifically as set out in the Enforcement Principle, they must provide (a) recourse for individuals to whom the data relate, (b) follow up procedures for verifying that the attestations and assertions they have made about their privacy practices are true, and (c) obligations to remedy problems arising out of failure to comply with the Principles and consequences for such organizations. An organization may satisfy points (a) and (c) of the Enforcement Principle if it adheres to the requirements of this FAQ for cooperating with the DPAs.

An organization may commit to cooperate with the DPAs by declaring in its Safe Harbor certification to the Department of Commerce (*see* FAQ 6: Self-Certification) that the organization:

1. Elects to satisfy the requirement in points (a) and (c) of the Safe Harbor Enforcement Principle by committing to cooperate with the DPAs;
2. Will cooperate with the DPAs in the investigation and resolution of complaints brought under the Safe Harbor; and
3. Will comply with any advice given by the DPAs where the DPAs take the view that the organization needs to take specific action to comply with the Safe Harbor Principles, including remedial or compensatory measures for the benefit of individuals affected by any non-compliance with the Principles, and will provide the DPAs with written confirmation that such action has been taken.

The cooperation of the DPAs will be provided in the form of information and advice in the following way:

- The advice of the DPAs will be delivered through an informal panel of DPAs established at the European Union level, which will *inter alia* help ensure a harmonized and coherent approach.
- The panel will provide advice to the U.S. organizations concerned on unresolved complaints from individuals about the handling of personal information that has been transferred from the EU under the Safe Harbor. This advice will be designed to ensure that the Safe Harbor Principles are being correctly applied and will include any remedies for the individual(s) concerned that the DPAs consider appropriate.
- The panel will provide such advice in response to referrals from the organizations concerned and/or to complaints received directly from individuals against organizations which have committed to cooperate with DPAs for Safe Harbor purposes, while encouraging and if necessary helping such individuals in the first instance to use the in-house complaint handling arrangements that the organization may offer.
- Advice will be issued only after both sides in a dispute have had a reasonable opportunity to comment and to provide any evidence they wish. The panel will seek to deliver advice as quickly as this requirement for due process allows. As a general rule, the panel will aim to provide advice within 60 days after receiving a complaint or referral and more quickly where possible.
- The panel will make public the results of its consideration of complaints submitted to it, if it sees fit.
- The delivery of advice through the panel will not give rise to any liability for the panel or for individual DPAs.

As noted above, organizations choosing this option for dispute resolution must undertake to comply with the advice of the DPAs. If an organization fails to comply within 25 days of the delivery of the advice and has offered no satisfactory explanation for the delay, the panel will give notice of its intention either to submit the matter to the Federal Trade Commission or other U.S. federal or state body with statutory

powers to take enforcement action in cases of deception or misrepresentation, or to conclude that the agreement to cooperate has been seriously breached and must therefore be considered null and void. In the latter case, the panel will inform the Department of Commerce (or its designee) so that the list of Safe Harbor participants can be duly amended. Any failure to fulfill the undertaking to cooperate with the DPAs, as well as failures to comply with the Safe Harbor Principles, will be actionable as a deceptive practice under Section 5 of the FTC Act or other similar statute.

Organizations choosing this option will be required to pay an annual fee which will be designed to cover the operating costs of the panel, and they may additionally be asked to meet any necessary translation expenses arising out of the panel's consideration of referrals or complaints against them. The annual fee will not exceed $500 and will be less for smaller companies.

The option of co-operating with the DPAs will be available to organizations joining the Safe Harbor during a three-year period. The DPAs will reconsider this arrangement before the end of that period if the number of U.S. organizations choosing this option proves to be excessive.

VI. Self-Certification

Q: How does an organization self-certify that it adheres to the Safe Harbor Principles?

A: Safe Harbor benefits are assured from the date on which an organization self-certifies to the Department of Commerce (or its designee) its adherence to the Principles in accordance with the guidance set forth below.

To self-certify for the Safe Harbor, organizations can provide to the Department of Commerce (or its designee) a letter – signed by a corporate officer on behalf of the organization that is joining the Safe Harbor – that contains at least the following information:

1. name of organization, mailing address, email address, telephone and fax numbers;
2. description of the activities of the organization with respect to personal information received from the EU; and description of the organization's privacy policy for such personal information, including:
    a. where the privacy policy is available for viewing by the public,
    b. its effective date of implementation,
    c. a contact office for the handling of complaints, access requests, and any other issues arising under the Safe Harbor,

d. the specific statutory body that has jurisdiction to hear any claims against the organization regarding possible unfair or deceptive practices and violations of laws or regulations governing privacy (and that is listed in the annex to the Principles),

e. name of any privacy programs in which the organization is a member,

f. method of verification (e.g. in-house, third party) (*see* FAQ 7: Verification) , and

g. the independent recourse mechanism that is available to investigate unresolved complaints.

Where the organization wishes its Safe Harbor benefits to cover human resources information transferred from the EU for use in the context of the employment relationship, it may do so where there is a statutory body with jurisdiction to hear claims against the organization arising out of human resources information that is listed in the annex to the Principles. In addition the organization must indicate this in its letter and declare its commitment to cooperate with the EU authority or authorities concerned in conformity with FAQ 9: Human Resources and FAQ 5: The Role of the Data Protection Authorities as applicable and that it will comply with the advice given by such authorities.

The Department (or its designee) will maintain a list of all organizations that file such letters, thereby assuring the availability of Safe Harbor benefits, and will update such list on the basis of annual letters and notifications received pursuant to FAQ 11: Dispute Resolution and Enforcement. Such self-certification letters should be provided not less than annually. Otherwise the organization will be removed from the list and Safe Harbor benefits will no longer be assured. Both the list and the self-certification letters submitted by the organizations will be made publicly available. All organizations that self-certify for the Safe Harbor must also state in their relevant published privacy policy statements that they adhere to the Safe Harbor Principles.

The undertaking to adhere to the Safe Harbor Principles is not time-limited in respect of data received during the period in which the organization enjoys the benefits of the Safe Harbor. Its undertaking means that it will continue to apply the Principles to such data for as long as the organization stores, uses or discloses them, even if it subsequently leaves the Safe Harbor for any reason.

An organization that will cease to exist as a separate legal entity as a result of a merger or a takeover must notify the Department of Commerce (or its designee) of this in advance. The notification should also indicate whether the acquiring entity or the entity resulting from the merger will

(1) continue to be bound by the Safe Harbor Principles by the operation of law governing the takeover or merger or (2) elect to self-certify its adherence to the Safe Harbor Principles or put in place other safeguards, such as a written agreement that will ensure adherence to the Safe Harbor Principles. Where neither (1) nor (2) applies, any data that has been acquired under the Safe Harbor must be promptly deleted.

An organization does not need to subject all personal information to the Safe Harbor Principles, but it must subject to the Safe Harbor Principles all personal data received from the EU after it joins the Safe Harbor.

Any misrepresentation to the general public concerning an organization's adherence to the Safe Harbor Principles may be actionable by the Federal Trade Commission or other relevant government body. Misrepresentations to the Department of Commerce (or its designee) may be actionable under the False Statements Act (18 U.S.C. § 1001).

VII. Verification

Q: How do organizations provide follow up procedures for verifying that the attestations and assertions they make about their Safe Harbor privacy practices are true and those privacy practices have been implemented as represented and in accordance with the Safe Harbor Principles?

A: To meet the verification requirements of the Enforcement Principle, an organization may verify such attestations and assertions either through self-assessment or outside compliance reviews.

Under the self-assessment approach, such verification would have to indicate that an organization's published privacy policy regarding personal information received from the EU is accurate, comprehensive, prominently displayed, completely implemented and accessible. It would also need to indicate that its privacy policy conforms to the Safe Harbor Principles; that individuals are informed of any in-house arrangements for handling complaints and of the independent mechanisms through which they may pursue complaints; that it has in place procedures for training employees in its implementation, and disciplining them for failure to follow it; and that it has in place internal procedures for periodically conducting objective reviews of compliance with the above. A statement verifying the self- assessment should be signed by a corporate officer or other authorized representative of the organization at least once a year and made available upon request by individuals or in the context of an investigation or a complaint about non-compliance.

Organizations should retain their records on the implementation of their Safe Harbor privacy practices and make them available upon request in the context of an investigation or a complaint about non-compliance to the independent body responsible for investigating complaints or to the agency with unfair and deceptive practices jurisdiction.

Where the organization has chosen outside compliance review, such a review needs to demonstrate that its privacy policy regarding personal information received from the EU conforms to the Safe Harbor Principles, that it is being complied with and that individuals are informed of the mechanisms through which they may pursue complaints. The methods of review may include without limitation auditing, random reviews, use of "decoys," or use of technology tools as appropriate. A statement verifying that an outside compliance review has been successfully completed should be signed either by the reviewer or by the corporate officer or other authorized representative of the organization at least once a year and made available upon request by individuals or in the context of an investigation or a complaint about compliance.

VIII. Access

Access Principle:

Individuals 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 legitimate rights of persons other than the individual would be violated.

Q1: Is the right of access absolute?

A1: No. Under the Safe Harbor Principles, the right of access is fundamental to privacy protection. In particular, it allows individuals to verify the accuracy of information held about them. Nonetheless, the obligation of an organization to provide access to the personal information it holds about an individual is subject to the principle of proportionality or reasonableness and has to be tempered in certain instances. Indeed, the Explanatory Memorandum to the 1980 OECD Privacy Guidelines makes clear that an organization's access obligation is not absolute. It does not require the exceedingly thorough search mandated, for example, by a subpoena, nor does it require access to all the different forms in which the information may be maintained by the organization.

Rather, experience has shown that in responding to individuals' access requests, organizations should first be guided by the concern(s) that led to the requests in the first place. For example, if an access request is vague or broad in scope, an organization may engage the individual in a dialogue so as to better understand the motivation for the request and to locate responsive information. The organization might inquire about which part(s) of the organization the individual interacted with and/or about the nature of the information (or its use) that is the subject of the access request. Individuals do not, however, have to justify requests for access to their own data.

Expense and burden are important factors and should be taken into account but they are not controlling in determining whether providing access is reasonable. For example, if the information is used for decisions that will significantly affect the individual (e.g., the denial or grant of important benefits, such as insurance, a mortgage, or a job), then consistent with the other provisions of these FAQs, the organization would have to disclose that information even if it is relatively difficult or expensive to provide.

If the information requested is not sensitive or not used for decisions that will significantly affect the individual (e.g., non-sensitive marketing data that is used to determine whether or not to send the individual a catalog), but is readily available and inexpensive to provide, an organization would have to provide access to factual information that the organization stores about the individual. The information concerned could include facts obtained from the individual, facts gathered in the course of a transaction, or facts obtained from others that pertain to the individual.

Consistent with the fundamental nature of access, organizations should always make good faith efforts to provide access. For example, where certain information needs to be protected and can be readily separated from other information subject to an access request, the organization should redact the protected information and make available the other information. If an organization determines that access should be denied in any particular instance, it should provide the individual requesting access with an explanation of why it has made that determination and a contact point for any further inquiries.

Q2: What is confidential commercial information and may organizations deny access in order to safeguard it?

A2: Confidential commercial information (as that term is used in the Federal Rules of Civil Procedure on discovery) is information which an organization has taken steps to protect from disclosure,

where disclosure would help a competitor in the market. The particular computer program an organization uses, such as a modeling program, or the details of that program may be confidential commercial information. Where confidential commercial information can be readily separated from other information subject to an access request, the organization should redact the confidential commercial information and make available the non-confidential information. Organizations may deny or limit access to the extent that granting it would reveal its own confidential commercial information as defined above, such as marketing inferences or classifications generated by the organization, or the confidential commercial information of another where such information is subject to a contractual obligation of confidentiality in circumstances where such an obligation of confidentiality would normally be undertaken or imposed.

Q3: In providing access, may an organization disclose to individuals personal information about them derived from its data bases or is access to the data base itself required?

A3: Access can be provided in the form of disclosure by an organization to the individual and does not require access by the individual to an organization's data base.

Q4: Does an organization have to restructure its data bases to be able to provide access?

A4: Access needs to be provided only to the extent that an organization stores the information. The access principle does not itself create any obligation to retain, maintain, reorganize, or restructure personal information files.

Q5: These replies make clear that access may be denied in certain circumstances. In what other circumstances may an organization deny individuals access to their personal information?

A5: Such circumstances are limited, and any reasons for denying access must be specific. An organization can refuse to provide access to information to the extent that disclosure is likely to interfere with the safeguarding of important countervailing public interests, such as national security; defense; or public security. In addition, where personal information is processed solely for research or statistical purposes, access may be denied. Other reasons for denying or limiting access are:

a. interference with execution or enforcement of the law, including the prevention, investigation or detection of offenses or the right to a fair trial;

b. interference with private causes of action, including the prevention, investigation or detection of legal claims or the right to a fair trial;

c. disclosure of personal information pertaining to other individual(s) where such references cannot be redacted;

d. breaching a legal or other professional privilege or obligation;

e. breaching the necessary confidentiality of future or ongoing negotiations, such as those involving the acquisition of publicly quoted companies;

f. prejudicing employee security investigations or grievance proceedings;

g. prejudicing the confidentiality that may be necessary for limited periods in connection with employee succession planning and corporate re-organizations; or

h. prejudicing the confidentiality that may be necessary in connection with monitoring, inspection or regulatory functions connected with sound economic or financial management; or

i. other circumstances in which the burden or cost of providing access would be disproportionate or the legitimate rights or interests of others would be violated.

An organization which claims an exception has the burden of demonstrating its applicability (as is normally the case). As noted above, the reasons for denying or limiting access and a contact point for further inquiries should be given to individuals.

Q6: Can an organization charge a fee to cover the cost of providing access?

A6: Yes. The OECD Guidelines recognize that organizations may charge a fee, provided that it is not excessive. Thus organizations may charge a reasonable fee for access. Charging a fee may be useful in discouraging repetitive and vexatious requests.

Organizations that are in the business of selling publicly available information may thus charge the organization's customary fee in responding to requests for access. Individuals may alternatively seek access to their information from the organization that originally compiled the data.

Access may not be refused on cost grounds if the individual offers to pay the costs.

Q7: Is an organization required to provide access to personal information derived from public records?

A7: To clarify first, public records are those records kept by government agencies or entities at any level that are open to consultation by the public in general. It is not necessary to apply the Access Principle to such information as long as it is not combined with other personal information, apart from when small amounts of non-public record information are used for indexing or organizing public record information. However, any conditions for consultation established by the relevant jurisdiction are to be respected. Where public record information is combined with other non-public record information (other than as specifically noted above), however, an organization must provide access to all such information, assuming it is not subject to other permitted exceptions.

Q8: Does the Access Principle have to be applied to publicly available personal information?

A8: As with public record information (*see* Q7), it is not necessary to provide access to information that is already publicly available to the public at large, as long as it is not combined with non-publicly available information.

Q9: How can an organization protect itself against repetitious or vexatious requests for access?

A9: An organization does not have to respond to such requests for access. For these reasons, organizations may charge a reasonable fee and may set reasonable limits on the number of times within a given period that access requests from a particular individual will be met. In setting such limitations, an organization should consider such factors as the frequency with which information is updated, the purpose for which the data are used, and the nature of the information.

Q10: How can an organization protect itself against fraudulent requests for access?

A10: An organization is not required to provide access unless it is supplied with sufficient information to allow it to confirm the identity of the person making the request.

Q11: Is there a time within which responses must be provided to access requests?

A11: Yes, organizations should respond without excessive delay and within a reasonable time period. This requirement may be satisfied in different ways as the explanatory memorandum to the 1980 OECD Privacy Guidelines states. For example, a data controller who provides information to data subjects at regular intervals may be exempted from obligations to respond at once to individual requests.

IX. Human Resources

Q1: Is the transfer from the EU to the United States of personal information collected in the context of the employment relationship covered by the Safe Harbor?

A1: Yes, where a company in the EU transfers personal information about its employees (past or present) collected in the context of the employment relationship, to a parent, affiliate, or unaffiliated service provider in the United States participating in the Safe Harbor, the transfer enjoys the benefits of the Safe Harbor. In such cases, the collection of the information and its processing prior to transfer will have been subject to the national laws of the EU country where it was collected, and any conditions for or restrictions on its transfer according to those laws will have to be respected.

The Safe Harbor Principles are relevant only when individually identified records are transferred or accessed. Statistical reporting relying on aggregate employment data and/or the use of anonymized or pseudonymized data does not raise privacy concerns.

Q2: How do the Notice and Choice Principles apply to such information?

A2: A U.S. organization that has received employee information from the EU under the Safe Harbor may disclose it to third parties and/or use it for different purposes only in accordance with the Notice and Choice Principles. For example, where an organization intends to use personal information collected through the employment relationship for non-employment-related purposes, such as marketing communications, the U.S. organization must provide the affected individuals with choice before doing so, unless they have already authorized the use of the information for such purposes. Moreover, such choices must not be used to restrict employment opportunities or take any punitive action against such employees.

It should be noted that certain generally applicable conditions for transfer from some Member States may preclude other uses of such information even after transfer outside the EU and such conditions will have to be respected.

In addition, employers should make reasonable efforts to accommodate employee privacy preferences. This could include, for example, restricting access to the data, anonymizing certain data, or assigning codes or pseudonyms when the actual names are not required for the management purpose at hand.

To the extent and for the period necessary to avoid prejudicing the legitimate interests of the organization in making promotions, appointments, or other similar employment decisions, an organization does not need to offer notice and choice.

Q3: How does the Access Principle apply?

A3: The FAQs on access provide guidance on reasons which may justify denying or limiting access on request in the human resources context. Of course, employers in the European Union must comply with local regulations and ensure that European Union employees have access to such information as is required by law in their home countries, regardless of the location of data processing and storage. The Safe Harbor requires that an organization processing such data in the United States will cooperate in providing such access either directly or through the EU employer.

Q4: How will enforcement be handled for employee data under the Safe Harbor Principles?

A4: In so far as information is used only in the context of the employment relationship, primary responsibility for the data *vis-à-vis* the employee remains with the company in the EU. It follows that, where European employees make complaints about violations of their data protection rights and are not satisfied with the results of internal review, complaint, and appeal procedures (or any applicable grievance procedures under a contract with a trade union), they should be directed to the state or national data protection or labor authority in the jurisdiction where the employee works. This also includes cases where the alleged mishandling of their personal information has taken place in the United States, is the responsibility of the U.S. organization that has received the information from the employer and not of the employer and thus involves an alleged breach of the Safe Harbor Principles,

rather than of national laws implementing the Directive. This will be the most efficient way to address the often overlapping rights and obligations imposed by local labor law and labor agreements as well as data protection law.

A U.S. organization participating in the Safe Harbor that uses EU human resources data transferred from the Europe Union in the context of the employment relationship and that wishes such transfers to be covered by the Safe Harbor must therefore commit to cooperate in investigations by and to comply with the advice of competent EU authorities in such cases. The DPAs that have agreed to cooperate in this way will notify the European Commission and the Department of Commerce. If a U.S. organization participating in the Safe Harbor wishes to transfer human resources data from a Member State where the DPA has not so agreed, the provisions of FAQ 5 will apply.

X. Article 17 Contracts

Q: When data is transferred from the EU to the United States only for processing purposes, will a contract be required, regardless of participation by the processor in the Safe Harbor?

A: Yes. 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. The purpose of the contract is to protect the interests of the data controller, i.e. the person or body who determines the purposes and means of processing, who retains full responsibility for the data *vis-à-vis* the individual(s) concerned. The contract thus specifies the processing to be carried out and any measures necessary to ensure that the data are kept secure.

A U.S. organization participating in the Safe Harbor and receiving personal information from the EU merely for processing thus does not have to apply the Principles to this information, because the controller in the EU remains responsible for it *vis-à-vis* the individual in accordance with the relevant EU provisions (which may be more stringent than the equivalent Safe Harbor Principles).

Because adequate protection is provided by Safe Harbor participants, contracts with Safe Harbor participants for mere processing do not require prior authorization (or such authorization will be granted automatically by the Member States) as would be required for contracts with recipients not participating in the Safe Harbor or otherwise not providing adequate protection.

XI. Dispute Resolution and Enforcement

Q: How should the dispute resolution requirements of the Enforcement Principle be implemented, and how will an organization's persistent failure to comply with the Principles be handled?

A: The Enforcement Principle sets out the requirements for Safe Harbor enforcement. How to meet the requirements of point (b) of the Principle is set out in the FAQ 7: Verification. This FAQ addresses points (a) and (c), both of which require independent recourse mechanisms. These mechanisms may take different forms, but they must meet the Enforcement Principle's requirements. Organizations may satisfy the requirements through the following:

1. Compliance with private sector developed privacy programs that incorporate the Safe Harbor Principles into their rules and that include effective enforcement mechanisms of the type described in the Enforcement Principle;
2. Compliance with legal or regulatory supervisory authorities that provide for handling of individual complaints and dispute resolution; or
3. Commitment to cooperate with data protection authorities located in the European Union or their authorized representatives.

This list is intended to be illustrative and not limiting. The private sector may design other mechanisms to provide enforcement, so long as they meet the requirements of the Enforcement Principle and the FAQs. Please note that the Enforcement Principle's requirements are additional to the requirement set forth in paragraph 3 of the introduction to the Principles that self-regulatory efforts must be enforceable under Article 5 of the Federal Trade Commission Act or similar statute.

Recourse Mechanisms:

Consumers should be encouraged to raise any complaints they may have with the relevant organization before proceeding to independent recourse mechanisms. Whether a recourse mechanism is independent is a factual question that can be demonstrated in a number of ways, for example, by transparent composition and financing or a proven track record. As required by the enforcement principle, the recourse available to individuals must be readily available and affordable. Dispute resolution bodies should look into each complaint received from individuals unless they are obviously unfounded or frivolous. This does not preclude the establishment of eligibility requirements by the organization

operating the recourse mechanism, but such requirements should be transparent and justified (for example to exclude complaints that fall outside the scope of the program or are for consideration in another forum), and should not have the effect of undermining the commitment to look into legitimate complaints. In addition, recourse mechanisms should provide individuals with full and readily available information about how the dispute resolution procedure works when they file a complaint. Such information should include notice about the mechanism's privacy practices, in conformity with the Safe Harbor Principles.[1] They should also co-operate in the development of tools such as standard complaint forms to facilitate the complaint resolution process.

Remedies and Sanctions:

The result of any remedies provided by the dispute resolution body should be that the effects of noncompliance are reversed or corrected by the organization, in so far as feasible, and that future processing by the organization will be in conformity with the Principles and, where appropriate, that processing of the personal data of the individual who has brought the complaint will cease. Sanctions need to be rigorous enough to ensure compliance by the organization with the Principles. A range of sanctions of varying degrees of severity will allow dispute resolution bodies to respond appropriately to varying degrees of non-compliance. Sanctions should include both publicity for findings of non-compliance and the requirement to delete data in certain circumstances.[2] Other sanctions could include suspension and removal of a seal, compensation for individuals for losses incurred as a result of non-compliance and injunctive orders. Private sector dispute resolution bodies and self-regulatory bodies must notify failures of Safe Harbor organizations to comply with their rulings to the governmental body with applicable jurisdiction or to the courts, as appropriate, and to notify the Department of Commerce (or its designee).

FTC Action:

The FTC has committed to reviewing on a priority basis referrals received from privacy self-regulatory organizations, such as BBBOnline and TRUSTe, and EU Member States alleging non-compliance with the Safe Harbor Principles to determine whether Section 5 of the FTC Act prohibiting unfair or deceptive acts or practices in commerce has been violated.

---

1. Dispute resolution bodies are not required to conform with the enforcement principle. They may also derogate from the Principles where they encounter conflicting obligations or explicit authorizations in the performance of their specific tasks.

2. Dispute resolutions bodies have discretion about the circumstances in which they use these sanctions. The sensitivity of the data concerned is one factor to be taken into consideration in deciding whether deletion of data should be required, as is whether an organization has collected, used or disclosed information in blatant contravention of the Principles.

If the FTC concludes that it has reason[s] to believe Section 5 has been violated, it may resolve the matter by seeking an administrative cease and desist order prohibiting the challenged practices or by filing a complaint in a federal district court, which if successful could result in a federal court order to same effect. The FTC may obtain civil penalties for violations of an administrative cease and desist order and may pursue civil or criminal contempt for violation of a federal court order. The FTC will notify the Department of Commerce of any such actions it takes. The Department of Commerce encourages other government bodies to notify it of the final disposition of any such referrals or other rulings determining adherence to the Safe Harbor Principles.

Persistent Failure to Comply:

If an organization persistently fails to comply with the Principles, it is no longer entitled to benefit from the Safe Harbor. Persistent failure to comply arises where an organization that has self-certified to the Department of Commerce (or its designee) refuses to comply with a final determination by any self-regulatory or government body or where such a body determines that an organization frequently fails to comply with the Principles to the point where its claim to comply is no longer credible. In these cases, the organization must promptly notify the Department of Commerce (or its designee) of such facts. Failure to do so may be actionable under the False Statements Act(18 U.S.C. § 1001).

The Department (or its designee) will indicate on the public list it maintains of organizations self-certifying adherence to the Safe Harbor Principles any notification it receives of persistent failure to comply, whether it is received from the organization itself, from a self-regulatory body, or from a government body, but only after first providing thirty (30) days' notice and an opportunity to respond to the organization that has failed to comply. Accordingly, the public list maintained by the Department of Commerce (or its designee) will make clear which organizations are assured and which organizations are no longer assured of Safe Harbor benefits.

An organization applying to participate in a self-regulatory body for the purposes of re-qualifying for the Safe Harbor must provide that body with full information about its prior participation in the Safe Harbor.

XII. Choice - Timing of Opt Out

Q: Does the Choice Principle permit an individual to exercise choice only at the beginning of a relationship or at any time?

A: Generally, the purpose of the Choice Principle is to ensure that personal information is used and disclosed in ways that are consistent with the individual's expectations and choices. Accordingly, an individual should be able to exercise "opt out" (or choice) of having personal information used for direct marketing at any time subject to reasonable limits established by the organization, such as giving the organization time to make the opt out effective. An organization may also require sufficient information to confirm the identity of the individual requesting the "opt out." In the United States, individuals may be able to exercise this option through the use of a central "opt out" program such as the Direct Marketing Association's Mail Preference Service. Organizations that participate in the Direct Marketing Association's Mail Preference Service should promote its availability to consumers who do not wish to receive commercial information. In any event, an individual should be given a readily available and affordable mechanism to exercise this option.

Similarly, an organization may use information 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.

XIII. Travel Information

Q: When can airline passenger reservation and other travel information, such as frequent flyer or hotel reservation information and special handling needs, such as meals to meet religious requirements or physical assistance, be transferred to organizations located outside the EU?

A: Such information may be transferred in several different circumstances. Under Article 26 of the Directive, personal data may be transferred "to a third country which does not ensure an adequate level of protection within the meaning of Article 25(2)" on the condition that it (1) is necessary to provide the services requested by the consumer or to fulfill the terms of an agreement, such as a "frequent flyer" agreement; or (2) has been unambiguously consented to by the consumer. U.S. organizations subscribing to the Safe Harbor provide adequate protection for personal data and may therefore receive data transfers from the EU without meeting those conditions or other conditions set out in Article 26 of the Directive. Since the Safe Harbor includes specific rules for sensitive information, such information

(which may need to be collected, for example, in connection with customers' needs for physical assistance) may be included in transfers to Safe Harbor participants. In all cases, however, the organization transferring the information has to respect the law in the EU Member State in which it is operating, which may *inter alia* impose special conditions for the handling of sensitive data.

XIV. Pharmaceutical and Medical Products

Q1: If personal data are collected in the EU and transferred to the United States for pharmaceutical research and/or other purposes, do Member State laws or the Safe Harbor Principles apply?

A1: Member State law applies to the collection of the personal data and to any processing that takes place prior to the transfer to the United States. The Safe Harbor Principles apply to the data once they have been transferred to the United States. Data used for pharmaceutical research and other purposes should be anonymized when appropriate.

Q2: Personal data developed in specific medical or pharmaceutical research studies often play a valuable role in future scientific research. Where personal data collected for one research study are transferred to a U.S. organization in the Safe Harbor, may the organization use the data for a new scientific research activity?

A2: Yes, if appropriate notice and choice have been provided in the first instance. Such a notice should provide information about any future specific uses of the data, such as periodic follow-up, related studies, or marketing. It is understood that not all future uses of the data can be specified, since a new research use could arise from new insights on the original data, new medical discoveries and advances, and public health and regulatory developments. Where appropriate, the notice should therefore include an explanation that personal data may be used in future medical and pharmaceutical research activities that are unanticipated. If the use is not consistent with the general research purpose(s) for which the data were originally collected, or to which the individual has consented subsequently, new consent must be obtained.

Q3: What happens to an individual's data if a participant decides voluntarily or at the request of the sponsor to withdraw from the clinical trial?

A3: Participants may decide or be asked to withdraw from a clinical trial at any time. Any data collected previous to withdrawal may still be processed along with other data collected as part of the clinical trial,

however, if this was made clear to the participant in the notice at the time he or she agreed to participate.

Q4: Pharmaceutical and medical device companies are allowed to provide personal data from clinical trials conducted in the EU to regulators in the United States for regulatory and supervision purposes. Are similar transfers allowed to parties other than regulators, such as company locations and other researchers?

A4: Yes, consistent with the Principles of Notice and Choice.

Q5: To ensure objectivity in many clinical trials, participants, and often investigators, as well, cannot be given access to information about which treatment each participant may be receiving. Doing so would jeopardize the validity of the research study and results. Will participants in such clinical trials (referred to as "blinded" studies) have access to the data on their treatment during the trial?

A5: No, such access does not have to be provided to a participant if this restriction has been explained when the participant entered the trial and the disclosure of such information would jeopardize the integrity of the research effort. Agreement to participate in the trial under these conditions is a reasonable forgoing of the right of access. Following the conclusion of the trial and analysis of the results, participants should have access to their data if they request it. They should seek it primarily from the physician or other health care provider from whom they received treatment within the clinical trial, or secondarily from the sponsoring company.

Q6: Does a pharmaceutical or medical device firm have to apply the Safe Harbor Principles with respect to notice, choice, onward transfer, and access in its product safety and efficacy monitoring activities, including the reporting of adverse events and the tracking of patients/subjects using certain medicines or medical devices (e.g. a pacemaker)?

A6: No, to the extent that adherence to the Principles interferes with compliance with regulatory requirements. This is true both with respect to reports by, for example, health care providers, to pharmaceutical and medical device companies, and with respect to reports by pharmaceutical and medical device companies to government agencies like the Food and Drug Administration.

Q7: Invariably, research data are uniquely key-coded at their origin by the principal investigator so as not to reveal the identity of individual data subjects.

Pharmaceutical companies sponsoring such research do not receive the key. The unique key code is held only by the researcher, so that he/she can identify the research subject under special circumstances (e.g. if follow-up medical attention is required). Does a transfer from the EU to the United States of data coded in this way constitute a transfer of personal data that is subject to the Safe Harbor Principles?

A7: No. This would not constitute a transfer of personal data that would be subject to the Principles.

XV. Public Record and Publicly Available Information

Q: Is it necessary to apply the Notice, Choice and Onward Transfer Principles to public record information or publicly available information?

A: It is not necessary to apply the Notice, Choice or Onward Transfer Principles to public record information, as long as it is not combined with non-public record information and as long as any conditions for consultation established by the relevant jurisdiction are respected.

Also, it is generally not necessary to apply the Notice, Choice or Onward Transfer Principles to publicly available information unless the European transferor indicates that such information is subject to restrictions that require application of those Principles by the organization for the uses it intends. Organizations will have no liability for how such information is used by those obtaining such information from published materials.

Where an organization is found to have intentionally made personal information public in contravention of the Principles so that it or others may benefit from these exceptions, it will cease to qualify for the benefits of the Safe Harbor.

Appendix A: Certification Form

Certifying an organization's adherence to the Safe Harbor

To expedite the certification process, prepare the required information before completing this form. If you have any difficulty completing this form or have any other questions concerning the Safe Harbor self-certification process, please e-mail or phone the International Trade Administration, Department of Commerce at safe.harbor@trade.gov or 202-482-4936.

Public reporting for this collection is estimated to range from 20 to 40 minutes per response, including the time for reviewing instructions, and completing and reviewing the collection of information. All responses to this collection of information are voluntary, and will be provided confidentially to the extent allowed under the Freedom of Information Act. Notwithstanding any other provisions of law, no person is required to respond to nor shall a person be subject to a penalty for failure to comply with a collection of information subject to the requirements of the Paperwork Reduction Act unless that collection of information displays a current valid OMB Control Number. Send comments regarding the burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to the Reports Clearance Officer, International Trade Administration, Department of Commerce, Room 4001, 14th and Constitution Avenue, N.W., Washington, D.C. 20230.

ORGANIZATION INFORMATION

Organization Name: _____

Address: _____

City: _____

State: _____

Zip: _____

Phone: _____

Fax: _____

Website (Optional):_____

ORGANIZATION CONTACT HANDLING COMPLAINTS, ACCESS REQUESTS, AND ANY OTHER ISSUE INVOLVING YOUR ORGANIZATION UNDER THE SAFE HARBOR FRAMEWORK(S)

Contact Office: _____

Contact Name (Optional):_____

Contact Title (Optional):_____

Contact Phone: _____

Contact Fax: _____

Contact Email: _____

CORPORATE OFFICER CERTIFYING YOUR ORGANIZATION'S ADHERENCE TO THE SAFE HARBOR FRAMEWORK(S)

Corporate Officer Name: _____

Corporate Officer Title: _____

Corporate Officer Phone: _____

Corporate Officer Fax: _____

Corporate Officer Email: _____

DESCRIPTION OF YOUR ORGANIZATION'S ACTIVITIES WITH RESPECT TO PERSONAL INFORMATION RECEIVED FROM THE EU / EEA AND / OR SWITZERLAND

DESCRIPTION OF YOUR ORGANIZATION'S PRIVACY POLICY FOR PERSONAL INFORMATION

Please enter the effective date of your organization's privacy policy:

Please provide the location of your organization's privacy policy:

OR

Upload the privacy policy:

Please indicate the appropriate statutory body that has jurisdiction to hear any claims against your organization regarding possible unfair or deceptive practices and violations of laws or regulations governing your organization's privacy practices:

Choose One: ☐ Federal Trade Commission (FTC) ☐ Department of Transportation

Please list any privacy programs in which your organization is a member for Safe Harbor purposes: **See FAQ 6**

What is your organization's verification method (e.g. In-house, Third Party?) **See FAQ 7**

What independent recourse mechanism(s) is(are) available to investigate unresolved complaints (e.g. private sector developed dispute resolution mechanism that incorporates the Safe Harbor Framework(s), the EU and/or Swiss data protection authorities)? See **U.S.-EU Safe Harbor Framework FAQ 11** and **U.S.-Swiss Safe Harbor Framework FAQ 11**

What personal data processed by your organization is covered by the Safe Harbor Framework(s)? (e.g. organization, client, customer, clinical trial data)? Please indicate whether or not the data covered includes manually processed data.

Does your organization plan to cover organization human resources data (i.e. personal information about your organization's employees, past or present, collected in the context of the employment relationship)? ☐ Yes ☐ No

If your organization does plan to cover organization human resources data, then it must agree to cooperate and comply with the EU and/or Swiss data protection authorities (See **U.S.-EU Safe Harbor Framework FAQ 5** and **FAQ 9** and **U.S.-Swiss Safe Harbor Framework FAQ 5** and **FAQ 9**). Does your organization agree to cooperate and comply with the appropriate data protection authorities?

☐ Yes ☐ No

Please select all of the listed countries from which your organization receives personal information.

Select All None

Austria	Estonia	Hungary	Liechtenstein	Norway	Slovenia
Belgium	Finland	Iceland	Lithuania	Poland	Spain
Bulgaria	France	Ireland	Luxembourg	Portugal	Sweden
Cyprus	Germany	Italy	Malta	Romania	Switzerland
Czech Republic	Greece	Latvia	Netherlands	Slovakia	United Kingdom
Denmark					

Please select your organization's appropriate Industry Sectors (Select up to 4)

Please select your organization's level of sales:

Please select your organization's number of employees:

Please print out your completed form now to verify that the information provided is correct and to retain a copy for your files.

If you are ready to submit the self-certification for your organization simply click the SUBMIT button below

SUBMIT

*See Appendix D for additional information

Appendix B: Sample Privacy Policies

Included below for your reference are three examples of privacy policies, which were chosen at random and are not intended to serve as an official endorsement or a specific U.S. Government standard. They incorporate the requisite tenets of the U.S.-EU Safe Harbor Framework while at the same time uniquely represent their individual company and their industry privacy concerns. Should you have any questions about what is required in the text of a privacy policy in order to be compliant with the U.S.-EU Safe Harbor Framework, please refer to the Helpful Hints on Self-Certifying Compliance.

Privacy Policy Example A

Data Privacy at XYZ XYZ has established a comprehensive privacy program, including a global privacy office and a chief privacy officer, designed to help us respect and protect your data privacy rights. This statement includes both XYZ's European Union - U.S. Safe Harbor Privacy Statement and the Website Privacy Statement.

U.S. - EU Safe Harbor Privacy Statement For personal information of employees, consumers, healthcare professionals, medical research subjects and investigators, customers, investors, and government officials that XYZ receives from the European Economic Area, XYZ has committed to handling such personal information in accordance with the Safe Harbor Principles. XYZ's Safe Harbor certification can be found at https://safeharbor.export.gov/list.aspx. For more information about the Safe Harbor Principles, please visit the U.S. Department of Commerce's Website at http://export.gov/safeharbor/.

XYZ Website Privacy Statement

XYZ respects the privacy of visitors to its websites, as a result, we have developed this website privacy policy. This website privacy policy applies only to the operation of websites that directly link to this policy when you click on "privacy statement" in the website footer. Through this website XYZ will collect information that can identify you, such as your name, address, telephone number, e-mail address, and other similar information ("Your Information") when it is voluntarily submitted to us (how-ever, see discussion below about "IP Addresses" if you have a broadband connection). We will use Your Information to respond to requests you may make of us, and from time to time, we may refer to Your Information to better understand your needs and how we can improve our websites, products and services.

We may also use Your Information to contact you and/or provide you with general health information (like information on certain health conditions) as well as information about our products and services. We may also enhance or merge Your Information with data obtained from third parties for the same purposes.

Any other information transferred by you in connection with your visit to this site ("Other Information" - that is, information that cannot be used to identify you) may be included in databases owned and maintained by XYZ or its agents. XYZ retains all rights to these databases and the information contained in them. Other Information we collect may include your IP Address and other information gathered through our weblogs and cookies (see below).

This site may use a technology known as **web beacons** - sometimes called single-pixel gifs - that allow this site to collect **web log** information. A web beacon is a graphic on a web page or in an e-mail message designed to track pages viewed or messages opened. Web log information is gathered when you visit one of our websites by the computer that hosts our website (called a "webserver"). The webserver automatically recognizes some non-personal information, such as the date and time you visited our site, the pages you visited, the website you came from, the type of browser you are using (e.g., Internet Explorer), the type of operating system you are using (e.g., Windows 2000), and the domain name and address of your Internet service provider (e.g., AOL). We may also include web beacons in promotional e-mail messages in order to determine whether messages have been opened.

This website may use a technology called a **"cookie"**. A cookie is a piece of information that our webserver sends to your computer (actually to your browser file) when you access a website. Then when you come back our site will detect whether you have one of our cookies on your computer. Our cookies help provide additional functionality to the site and help us analyze site usage more accurately. For instance, our site may set a cookie on your browser that keeps you from needing to remember and then enter a password more than once during a visit to the site.

This website uses Internet Protocol (IP) Addresses. An IP Address is a number assigned to your computer by your Internet service provider so you can access the Internet. Generally, an IP address changes each time you connect to the Internet (it is a "dynamic" address). Note, however, that if you have a broadband connection, depending on your individual circumstance, it is possible that your IP Address

that we collect, or even perhaps a cookie we use, may contain information that could be deemed identifiable. This is because with some broadband connections your IP Address doesn't change (it is "static") and could be associated with your personal computer. We use your IP address to report aggregate information on use and to help improve the website.

You should be aware that this site is not intended for, or designed to attract, individuals under the age of 18. We do not collect personally identifiable information from any person we actually know is an individual under the age of 18.

Areas of this website that collect Your Information use industry standard secure socket layer encryption (SSL); however, to take advantage of this your browser must support encryption protection (found in Internet Explorer release 3.0 and above).

We may share Your Information with agents, contractors or partners of XYZ in connection with services that these individuals or entities perform for, or with, XYZ. These agents, contractors or partners are restricted from using this data in any way other than to provide services for XYZ, or services for the collaboration in which they and XYZ are engaged (for example, some of our products are developed and marketed through joint agreements with other companies). We may, for example, provide your information to agents, contractors or partners for hosting our databases, for data processing services, or so that they can mail you information that you requested.

XYZ reserves the right to share Your Information to respond to duly authorized information requests of governmental authorities or where required by law. In exceptionally rare circumstances where national, state or company security is at issue (such as with the World Trade Center terrorist act in September, 2001), XYZ reserves the right to share our entire database of visitors and customers with appropriate governmental authorities.

We may also provide Your Information to a third party in connection with the sale, assignment, or other transfer of the business of this website to which the information relates, in which case we will require any such buyer to agree to treat Your Information in accordance with this Privacy Policy.

As a convenience to our visitors, this Website currently contains links to a number of sites that we believe may offer useful information. The policies and procedures we described here do not apply to those sites. We suggest contacting those sites directly for information on their privacy, security, data collection, and distribution policies.

To be removed from our contact lists, please write to XYZ at the following address:

XYZ
P.O. Box ####

City, State Zip Code

Please note that you may continue to receive materials while we are updating our lists.

We may update this Web site Privacy Policy from time to time. When we do update it, for your convenience, we will make the updated policy available on this page.

Last Updated: January 1, 2008

Privacy Policy Example B

XYZ Safe Harbor Policy

Introduction

XYZ, Inc. (the "Company") is a leading pure-play managed services provider that offers security assessment, detection and prevention services that help companies, governments and organizations safeguard their computer networks and systems. Protecting consumer privacy is important to the Company. The Company and its affiliated United States subsidiaries (hereinafter collectively referred to as the "Company," "we," "us" or "our") adhere to the Safe Harbor Agreement concerning the transfer of personal data from the European Union ("EU") to the United States of America. Accordingly, we follow the Safe Harbor Principles published by the U.S. Department of Commerce (the "Principles") with respect to all such data. If there is any conflict between the policies in this privacy policy and the Principles, the Principles shall govern. This privacy policy outlines our general policy and practices for implementing the Principles, including the types of information we gather, how we use it and the notice and choice affected individuals have regarding our use of and their ability to correct that information. This privacy policy applies to all personal information received by the Company whether in electronic, paper or verbal format.

Definitions

"Personal Information" or "Information" means information that (1) is transferred from the EU to the United States; (2) is recorded in any form; (3) is about, or pertains to a specific individual; and (4) can be linked to that individual.

“Sensitive Personal Information” means personal information that reveals race, ethnic origin, sexual orientation, political opinions, religious or philosophical beliefs, trade union membership or that concerns an individual’s health.

Principles

Notice

Company shall inform an individual of the purpose for which it collects and uses the Personal Information and the types of non-agent third parties to which the Company discloses or may disclose that Information. Company shall provide the individual with the choice and means for limiting the use and disclosure of their Personal Information. Notice will be provided in clear and conspicuous language when individuals are first asked to provide Personal Information to the Company, or as soon as practicable thereafter, and in any event before the Company uses or discloses the Information for a purpose other than for which it was originally collected.

Choice

The Company will offer individuals the opportunity to choose (opt out) whether their Personal Information is (1) to be disclosed to a third party or (2) to be used for a purpose other than the purpose for which it was originally collected or subsequently authorized by the individual. For Sensitive Personal Information, the Company will give individuals the opportunity to affirmatively or explicitly (opt out) consent to the disclosure of the information for a purpose other than the purpose for which it was originally collected or subsequently authorized by the individual. Company shall treat Sensitive Personal Information received from an individual the same as the individual would treat and identify it as Sensitive Personal Information.

Onward Transfers

Prior to disclosing Personal Information to a third party, Company shall notify the individual of such disclosure and allow the individual the choice (opt out) of such disclosure. Company shall ensure that any third party for which Personal Information may be disclosed subscribes to the Principles or are subject to law providing the same level of privacy protection as is required by the Principles and agree in writing to provide an adequate level of privacy protection.

Data Security

Company shall take reasonable steps to protect the Information from loss, misuse and unauthorized access, disclosure, alteration and destruction. Company has put in place appropriate physical, electronic and managerial procedures to safeguard and secure the Information from loss, misuse,

unauthorized access or disclosure, alteration or destruction. Company cannot guarantee the security of Information on or transmitted via the Internet.

Data Integrity

Company shall only process Personal Information in a way that is compatible with and relevant for the purpose for which it was collected or authorized by the individual. To the extent necessary for those purposes, Company shall take reasonable steps to ensure that Personal Information is accurate, complete, current and reliable for its intended use.

Access

Company shall allow an individual access to their Personal Information and allow the individual to correct, amend or delete inaccurate information, except where the burden or expense of providing access would be disproportionate to the risks to the privacy of the individual in the case in question or where the rights of persons other than the individual would be violated.

Enforcement

Company uses a self-assessment approach to assure compliance with this privacy policy and periodically verifies that the policy is accurate, comprehensive for the information intended to be covered, prominently displayed, completely implemented and accessible and in conformity with the Principles. We encourage interested persons to raise any concerns using the contact information provided and we will investigate and attempt to resolve any complaints and disputes regarding use and disclosure of Personal Information in accordance with the Principles.

If a complaint or dispute cannot be resolved through our internal process, we agree to dispute resolution using (an independent resource mechanism) as a third party resolution provider.

Amendments

This privacy policy may be amended from time to time consistent with the requirements of the Safe Harbor. We will post any revised policy on this website.

Information Subject to Other Policies

The Company is committed to following the Principles for all Personal Information within the scope of the Safe Harbor Agreement. However, certain information is subject to policies of the Company that may differ in some respects from the general policies set forth in this privacy policy.

Contact Information

Questions, comments or complaints regarding the Company's Safe Harbor Policy or data collection and processing practices can be mailed or emailed to:

XYZ
Attn: Legal Department
PO Box ####
City, State Zip

Effective date: January 1, 2008

Privacy Policy Example C

To learn more about our privacy practices, see our Privacy Policy Details.

XYZ believes in protecting your privacy. When we collect personal information from you on our website, we follow the privacy principles of (an independent resource mechanism) and comply with the U.S.-EU Safe Harbor Framework as set forth by the U.S. Department of Commerce regarding the collection, use and retention of personal data from the European Union. These are our promises to you:

1. Notice. When we collect your personal information, we'll give you timely and appropriate notice describing what personal information we're collecting, how we'll use it, and the types of third parties with whom we may share it.

2. Choice. We'll give you choices about the ways we use and share your personal information, and we'll respect the choices you make.

3. Relevance. We'll collect only as much personal information as we need for specific, identified purposes, and we won't use it for other purposes without obtaining your consent.

4. Retention. We'll keep your personal information only as long as we need it for the purposes for which we collected it, or as permitted by law.

5. Accuracy. We'll take appropriate steps to make sure the personal information in our records is accurate.

6. Access. We'll provide ways for you to access your personal information, as required by law, so you can correct inaccuracies.

7. Security. We'll take appropriate physical, technical, and organizational measures to protect your personal information from loss, misuse, unauthorized access or disclosure, alteration, and destruction.

8. Sharing. Except as described in this policy, we won't share your personal information with third parties without your consent.

9. International Transfer. If we transfer your personal information to another country, we'll take appropriate measures to protect your privacy and the personal information we transfer.

10. Enforcement. We'll regularly review how we're meeting these privacy promises, and we'll provide an independent way to resolve complaints about our privacy practices.

To access your information, ask questions about our privacy practices, or issue a complaint, contact us at:

XYZ
PO Box ####
City, State Zip (###) ###-####
Email Address

If your inquiry is not satisfactorily addressed, contact the (an independent resource mechanism) Dispute Resolution Process. (an independent resource mechanism) will serve as a liaison with the website to resolve your concerns.

To learn more about our privacy practices, see our Privacy Policy details.

Appendix C: Dispute Resolution and Enforcement Options

Under the Safe Harbor Enforcement Principle, organizations self-certifying to one or both of the Safe Harbor Frameworks must establish an independent recourse mechanism (i.e. third party dispute resolution provider) to investigate unresolved complaints. An organization wishing to self-certify must ensure that a suitable mechanism is in place prior to self-certification.

If an organization's self-certification covers human resources data received from EU/EEA and/or Switzerland regarding its own employees (i.e. organization human resources data, as opposed to customer/client human resources data), then it must agree to cooperate and comply with the EU data protection authorities (DPAs) and/or the Swiss Federal Data Protection and Information Commissioner (FDPIC) with respect to such data.

Provision has also been made for organizations to choose, even where organization human resources data are not involved, to cooperate with the appropriate data protection authorities in order to satisfy the Enforcement Principle's dispute resolution and remedy requirements.

In short, where an organization's self-certification does not cover organization human resources data it may meet the relevant requirements by:

a) Putting in place a suitable private sector developed mechanism; or

b) Cooperating and complying with the appropriate data protection authorities

In contrast, where an organization's self-certification does cover organization human resources data it may meet the relevant requirements by:

a) Cooperating and complying with the appropriate data protection authorities with respect to all types of data; or

b) Cooperating and complying with the appropriate data protection authorities exclusively with respect to organization human resources data and using a suitable private sector developed mechanism for all other types of data (e.g. customer/client, clinical trial, etc.)

Although private sector developed mechanisms vary, the specific mechanism chosen must consist of either:

a) A mechanism provided as part of a program, such as those managed by the Council of Better Business Bureaus (BBB), TRUSTe or Direct Marketing Association (DMA), that incorporates the Safe Harbor Framework; or

b) An outside arbitration and mediation mechanism, such as those offered by the American Arbitration Association (AAA) and JAMS, that agrees to hear each complaint in compliance with the Safe Harbor Framework

The following private sector organizations provide dispute resolution programs that assist in compliance with the Safe Harbor Enforcement Principle:

- BBB EU Safe Harbor: http://www.bbb.org/us/european-dispute-resolution/
- TRUSTe: http //www.truste.com/
- Direct Marketing Association (DMA) Safe Harbor: http://www.dmaresponsibility.org/SafeHarbor/
- AICPA WebTrust: www.aicpa.org/trustservices/
- Entertainment Software Rating Board: www.esrb.org/
- American Arbitration Association: http://www.adr.org/drs
- JAMS: http://www.jamsadr.com/

The list provided above is not exhaustive, and the Department of Commerce does not require or endorse any particular program.

Included below are descriptions of three representative private sector dispute resolution organizations (BBB, TRUSTe, and DMA) and the services that they offer.

BBB EU Safe Harbor Dispute Resolution Procedure

The Council of Better Business Bureaus ("BBB") is an unbiased organization that fosters honest and responsive relationships between businesses and consumers– instilling consumer confidence and contributing to a trustworthy marketplace. BBB provides objective advice, free business Reliability Reports and charity Wise Giving Reports, and educational information on topics affecting marketplace trust. To further promote trust, BBB also offers complaint and dispute resolution support for consumers and businesses when there is difference in viewpoints.

The BBB EU Safe Harbor Dispute Resolution Procedure ("Procedure") fulfills the dispute resolution mechanism requirement of the Department of Commerce's Safe Harbor Certification Program. As a recognized leader in business-to-consumer dispute resolution programs, the BBB provides for the review of complaints filed by EU citizens alleging that a business participating in the Procedure has failed to comply with the Safe Harbor Privacy Principles.

In the event that the BBB Procedure receives a complaint from an EU citizen, the first step in the dispute resolution process is for the BBB Procedure to contact the business. The BBB Procedure will ensure that the complainant has made a good faith effort to resolve his or her claim directly with the business, and then will attempt an informal mediation between the EU citizen and the business with the goal of rectifying the EU citizen's concern.

If the BBB Procedure is unable to address the EU citizen's concerns informally with the business, the second step is the more formal Data Privacy Review ("Review"). In the Review, the complainant submits a statement of his or her complaint, which is forwarded to the business. The business replies with an answer. Each party has one further opportunity to respond. When all information has been submitted, the BBB Procedure reviews the information and will issue a decision. If appropriate, the BBB Procedure will recommend corrective action to the business to ensure that all Safe Harbor Privacy Principles are met.

The third step in the Procedure is the Data Privacy Appeal. Both parties have the right to appeal the Review decision. In the event of an appeal, the case will be forwarded by the BBB to an independent expert in the privacy field. The appeal will be determined by the expert, who will issue a final decision in the case.

To register for participation in the BBB EU Safe Harbor Dispute Resolution Procedure, please visit us at us.bbb.org. Click on BBB For Businesses, and, under Programs and Services, BBB EU Safe Harbor (see also: http://www.bbb.org/us/european-dispute-resolution/getting-started/). For more information, please contact us at 800-334-2406 or email eusafeharbor@council.bbb.org.

TRUSTe Dispute Resolution Program

TRUSTe provides a broad suite of privacy services to help businesses build trust and increase engagement across all of their online channels - including websites, mobile applications, advertising, cloud services, business analytics and email marketing.

TRUSTe provides the following services to clients interested in self-certifying compliance with the U.S.-EU Safe Harbor Framework and/or the U.S. Swiss Safe Harbor Framework: verification of the client's compliance with the one or both of the Safe Harbor Frameworks, dispute resolution of consumer complaints about data collected on-line or off-line, and assistance in getting ready for self-certification with the U.S. Department of Commerce.

The TRUSTe Dispute Resolution program provides free online third-party privacy dispute resolution to anyone who files an eligible complaint about a TRUSTe certified client or client that has purchased Dispute Resolution services. TRUSTe reviews all such complaints; however, TRUSTe is not obligated to pursue any complaint that it deems frivolous or that constitutes harassment of either TRUSTe or a TRUSTe client.

While TRUSTe's final determination is not binding on the individual, the client must comply with TRUSTe's final determination or face removal from the TRUSTe program, possible publication of that removal, and/or referral to an appropriate law-enforcement body.

For sales, consumer, and press inquiries, please visit us at http://www.truste.com/about-TRUSTe/contact_us.

Direct Marketing Association Member Safe Harbor Program

The DMA provides technical assistance and extensive educational materials available on the DMA website: www.the-dma.org/safeharbor.

How Can the DMA Safe Harbor Program Assist Its Participating Member Companies?

- The DMA serves as a third-party dispute and enforcement mechanism for unresolved European data privacy complaints (The DMA has at least four decades of experience in addressing and satisfactorily resolving consumer disputes);
- Each participant receives a staff review of the company's Safe Harbor privacy policy statement; and
- The DMA provides a DMA Safe Harbor Program mark that companies can display on their relevant online or offline materials.

Who is eligible to participate in the DMA Safe Harbor Program?

The DMA Safe Harbor Program is only available to DMA Members. DMA companies wishing to participate in our Safe Harbor program must submit an application which includes: a signed contract, company contact sheet, copy of their Safe Harbor privacy policy statement and annual Safe Harbor fee.

Questions?

If you would like to join DMA or have questions regarding membership then please contact our membership team at: 212.768.7277 ext. 1155, membership@the-dma.org, or www.the-dma.org/aboutdma/benefitsofjoining.shtml.

Appendix D: U.S.-Swiss Safe Harbor Framework

The Swiss Federal Act on Data Protection (FADP) went into effect in July 1993, followed by important modifications in January 2008. The FADP would prohibit the transfer of personal data to countries that do not meet Switzerland's "adequacy" standard for privacy protection. While the United States and Switzerland share the goal of enhancing privacy protection for their citizens, the United States takes a different approach to privacy from that taken by Switzerland. The United States uses a sectoral approach that relies on a mix of legislation, regulation, and self-regulation. Switzerland, however, relies on comprehensive legislation that requires, among other things, the creation of an independent government data protection agency, registration of databases with this agency, and in some instances prior approval before personal data processing may begin. As a result of these different privacy approaches, the FADP could have significantly hampered the ability of U.S. organizations to engage in a range of trans-Atlantic transactions.

In order to bridge these differences in approach and provide a streamlined means for U.S. organizations to comply with the FADP, the U.S. Department of Commerce in consultation with the Federal Data Protection and Information Commissioner of Switzerland developed a "safe harbor" framework. The U.S.-Swiss Safe Harbor Framework, which was approved by Switzerland in 2009, is an important way for U.S. organizations to avoid experiencing interruptions in their business dealings with Switzerland or facing prosecution by Swiss authorities under Swiss privacy law. Self-certifying to the U.S.-Swiss Safe Harbor Framework will ensure that Swiss organizations know that your organization provides "adequate" privacy protection, as defined by Swiss law.

An organization does not have to self-certify compliance with the U.S.-EU Safe Harbor Framework in order to self-certify compliance with the U.S.-Swiss Safe Harbor Framework and vice versa. Although the respective sets of Safe Harbor Privacy Principles, frequently asked questions and answers (FAQs), and enforcement statements of the two Safe Harbor Frameworks are similar, they differ in a number of ways. Understanding the Safe Harbor Frameworks requires familiarity with all of the relevant documents.

The certification form used for self-certifying compliance with the U.S.-EU Safe Harbor Framework is identical to that used for self-certifying compliance with the U.S.-Swiss Safe Harbor Framework; therefore, an organization may self-certify to one or both of the Safe Harbor Frameworks when self-certifying via the Safe Harbor website. Organizations should note that when they select "Switzerland" as a country from which they receive personal data (i.e. whether they specifically ticked the box corresponding to "Switzerland" or used the "All" function), they are self-certifying compliance with the U.S.-Swiss Safe Harbor Framework. If an organization selects Switzerland, then the relevant privacy policy must make specific reference to the U.S.-Swiss Safe Harbor Framework, regardless of whether the organization has also self-certified its compliance with the U.S.-EU Safe Harbor Framework.

Appendix E: Safe Harbor Certification mark

On July 31, 2008, the International Trade Administration (ITA) announced that it developed a certification mark for the U.S.-European Union (EU) Safe Harbor Framework. The mark may be used by organizations on their websites to signify that they have self-certified compliance with the provisions of the U.S.-EU Safe Harbor Framework.

The U.S.-EU Safe Harbor Framework facilitates secure, uninterrupted transfers of personal information that support billions of dollars in trade from the EU to the United States. By displaying this certification mark, participating organizations can more easily illustrate their commitment to ensuring that EU citizens' data is secure, which is critical to the U.S.-EU trade relationship.

In order to display the certification mark, participating U.S. organizations must follow specific instructions developed by ITA. Only those organizations that have self-certified and are listed on ITA's official Safe Harbor Program list will be allowed to use the mark in an appropriate manner. Continued use of the mark is contingent on companies maintaining their status in the program.

Instructions for Self-Certified Organizations on the use of the Safe Harbor Certification mark

Congratulations on your self-certification to the U.S.-EU Safe Harbor Framework. Your self-certification is valid for one year and is renewable annually on or before your anniversary of enrolling in the Framework. In order to continue to take advantage of the benefits that self-certification affords, you must maintain your official filing and inform the Department of any changes in the scope of your organization's activities within the European Union. The Department provides its "Safe Harbor" certification mark (referred to hereafter as "mark") to those organizations that maintain their "current" status by self-certifying their practices in an official, annual filing with the Department. This mark must be used in accordance with the following instructions.

Safe Harbor Certification Mark Instructions

1. The mark is a visual manifestation of the commitment your organization makes when it self-certifies that it will comply with the U.S.-EU Safe Harbor Framework.

2. Your organization may announce its self-certification in a press release and include the mark as evidence that it has met the self-certification requirements established by the Department for the U.S.-EU Safe Harbor Framework.

3. Your organization may use the mark for one year from the initial self-certification date. Authorization to use the mark is renewable each year subject to the organization's reaffirmation to comply with the Safe Harbor Framework.

4. The mark may not be used for marketing or advertisements, and/or to imply any endorsement, authorization, or affiliation that does not exist with respect to the U.S. Department of Commerce or the United States Government.

5. The mark may not be used in a manner that embarrasses the Department or the United States Government.

6. The mark may be placed on the organization's website on its home page or on the page where the privacy policy is found.

7. In each instance in which you post the mark on your organization's website, you must:

a) Immediately above the top edge of the mark, display the following language, in a clear and conspicuous manner not to exceed the width of the mark in a minimum 8 point font, "We self-certify compliance with". With the words "We self-certify compliance with", provide a link to:

http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+list

b) With the mark, provide a link to: www.export.gov/safeharbor

8. The mark must be removed from the organization's website under the appropriate circumstances including, but not limited to: a. the organization withdraws from participation or is removed as a participant in the U.S.-EU Safe Harbor Framework; b. the organization fails to comply with a final ruling of a private sector dispute resolution body, a self-regulatory body, or government body, as applicable, in connection with allegations of Safe Harbor non-compliance; c. the organization fails to renew its commitment to the Framework in a reasonable time and in accordance with the reaffirmation requirements; d. the organization is acquired by another entity that either is not in the Framework or chooses to opt-out of the program; or e. the organization ceases commercial operations.

9. Failure to comply with these instructions may result in enforcement of the certification mark through an action for infringement of the mark, and/or a referral to the Federal Trade Commission for investigation of an unfair or deceptive trade practice under section 5 of the Federal Trade Commission Act.

Appendix F: Glossary*

Access – The ability to view personal information held by an organization – this ability may be complemented by an ability to update or correct the information. Access defines the intersection of identity and data; that is, who can do what to which data.

Adequacy – Adequacy refers to the recognition of the existence of a legal regime in another country that provides sufficient protection for personal information. As used in the EU Data Protection Directive, a country will be deemed "adequate" if its laws afford individuals rights that are similar to those afforded by the EU Data Protection Directive. In the EU context, if a country offers adequate protection, then data transfers from the European Economic Area (EEA) to that country may occur without any further limitation – provided that the processing meets the other provisions of the EU Directive. The adequacy concept has been expanded to encompass other types of data transfer mechanisms. For example, the U.S.-EU Safe Harbor Framework provides an adequate level of protection, so organizations that are in the Safe Harbor program may transfer data from the European Union to the United States. Similarly, the EU standard contractual clauses provide an adequate level of protection, so data may be transferred from the EU to any country, if the recipient has executed a contract that incorporates the standard contractual clauses.

Choice – An individual's ability to determine whether or how personal information collected from him or her may be used or disclosed by the entity that collected the information. Also: The ability of an individual to limit certain uses of his or her personal information. For example, an individual may have choice about whether to permit a organization to contact the individual or share the individual's data with third parties.

Data commissioner – Government official that runs a data protection office and that is charged with enforcing a country's data protection laws.

Data controller – A controller is any person who makes decisions with regard to the processing of personal data, including decisions about the *purposes* for which the personal data are processed and the *manner* in which the personal data are processed. The EU Directive defines a data "controller" as: "the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or community law."

Data processor – A data processor is a person who processes the data on behalf of the data controller, but who is under the authority of the data controller. The EU Directive defines data "processor" as: "a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller."

Data protection – The management of personal information. In the United States, "privacy" is the term that is used in policies, laws, and regulations. In contrast, in Switzerland, the European Union, and other countries, the term "data protection" often identifies privacy-related laws and regulations.

Data protection authority – *See* also Data protection office, Data commissioner.

Data protection office – A government agency that enforces data protection legislation. According to the EU Directive: "Each member state shall provide that one or more public authorities are responsible for monitoring the application within its territory of the provisions adopted by the member states pursuant to this Directive. These authorities shall act with complete independence in exercising the functions entrusted to them. Each authority has investigative powers necessary for the performance of its supervisory duties, power to engage in legal proceedings in case of violations. Each supervisory authority shall hear claims lodged by any person, or by an association representing that person." *See* also Data protection authority, Data commissioner.

Data subject – Term used in some data protection litigation to describe an individual who is the subject of a personal data record.

Deceptive trade practices – In the context of U.S. federal law, a term associated with corporate entities that mislead or misrepresent products or services to consumers and customers. These practices are regulated by the Federal Trade Commission at the federal level and typically by the Attorney General's Office of Consumer Protection at the state level. These laws typically provide both for enforcement by the government to stop the practice and individual actions for damages brought by consumers who are hurt by the practices.

Dispute resolution – The response to a valid complaint or grievance, or the action taken to correct faulty information, or to make amends for harm or inconvenience caused to an individual.

EU Data Protection Directive (EU Directive) – Several directives deal with personal data usage, but the most important is the general policy approved by the European Commission in 1995 (95/46/EC) which protects individuals' privacy and personal data use. The EU Directive was adopted in 1995 and became effective in 1998. The EU Directive recognizes the European view that privacy is a fundamental human right, and establishes a general comprehensive legal framework that is aimed at protecting individuals and promoting individual choice regarding the processing of personal data. The EU Directive imposes an onerous set of requirements on any person that collects or processes data pertaining to individuals in their personal or professional capacity. It is based on a set of data protection principles, which include the legitimate basis, purpose limitation, data quality, proportionality, and transparency principles, data security and confidentiality, data subjects' rights of access, rectification, deletion, and objection, restrictions on onwards transfers, additional protection where special categories of data and direct marketing are involved, and a prohibition on automated individual decisions. The EU Directive applies to all sectors of industry, from financial institutions to consumer goods companies, and from list brokers to any employer. The EU Directive's key provisions impose serious restrictions on personal data processing, grant individual rights to "data subjects," and set forth specific procedural obligations, including notification to national authority.

European Economic Area (EEA)◊ – The EEA allows Iceland, Liechtenstein, and Norway to participate in the EU's internal market without a conventional EU membership. These three countries apply EEA law, which is identical to all EU legislation related to the single market, with the exception of legislation on agriculture, fisheries, and fiscal issues. The EEA, however, is not a customs union. Switzerland is not a member of the EEA, but has concluded a large number of bilateral agreements with the EU covering a significant part of EEA law.

European Union (EU) – The European Union is an organization of European countries dedicated to increasing economic integration and strengthening cooperation among its members. The European Union was involved in the development of the Safe Harbor Principles that affect data flows from the European Union into the United States. As of July 2008, the member states include: Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, and United Kingdom.

Federal Trade Commission (FTC) – The U.S. Federal Trade Commission enforces a variety of federal antitrust and consumer protection laws, including the Safe Harbor Principles. The FTC seeks to ensure that the nation's markets function competitively, and are vigorous, efficient, and free of undue restrictions. The FTC also works to enhance the smooth operation of the marketplace by eliminating acts or practices that are unfair or deceptive.

Member state – In EU documents, this term refers to a country that is a full member of the European Union. *See* European Union.

Notice – A written description of an entity's practices with respect to its collection, use and disclosure of personal information. A private notice typically includes a description of what personal information the entity collects, how the entity uses the information, with whom it shares the information, whether the information is secured, and whether an individual has any choices as to how the entity uses the information.

Opt-in – A consumer's expression of affirmative consent based upon a specific act of the consumer.

Opt-out – A consumer's exercise of choice through an affirmative request that a particular use of disclosure of data not occur.

Personal data – The EU Directive defines "personal data" as: "any information relating to an identified or identifiable natural person ('data subject')" and explains that an "identifiable person" is "one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity."

Personal information – Any information that (i) relates to an individual and (ii) identifies or can be used to identify the individual. Such information may include an individual's name, postal address, e-mail address, telephone number, Social Security number, or other unique identifier.

Privacy – The appropriate use of personal information under the circumstances. What is appropriate will depend on context, law, and the individual's expectations; also, the right of an individual to control the collection, use, and disclosure of personal information.

Privacy policy – An organization's standard pertaining to the user information it collects and what is done with the information after it is collected.

Privacy seal program – Self-regulatory regimes that certify compliance with a set of standards of privacy protection. Services provide a "trust" mark, as well as independent verification and remediation and dispute resolution mechanisms for online privacy practices. Websites display the program's seal to indicate that they adhere to these standards.

Privacy statement – An organization's communication regarding its privacy policies, such as what personal information is collected, how it will be used, with whom it will be shared, and whether one has the option to exercise control over how one's information is used. Privacy statements are frequently posted on websites.

Processing of personal data – The EU Directive defines "processing" as: "any operation or set of operations performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure, or destruction."

Safe Harbor – The EU Directive and the Swiss Federal Act on Data Protection (FADP) prohibit the transfer of personal data outside of the European Union and Switzerland respectively, to jurisdictions that do not meet the European "adequacy" standard for privacy protection. While the United States, the European Union, and Switzerland share the goal of privacy protection, the United States uses a sectoral approach that relies on a mix of legislation, regulation, and self-regulation, while the European Union and Switzerland rely on comprehensive legislation that requires, among other things, the creation of government data protection agencies. As a result of these different approaches to privacy protection, the EU Directive and the FADP could have significantly hampered the ability of U.S. organizations to engage in many trans-Atlantic transactions.

In order to bridge the differences in approach and provide a streamlined means for U.S. organizations to comply with the EU data protection requirements, the U.S. Department of Commerce and the European Commission developed a "Safe Harbor" framework. The U.S.-EU Safe Harbor Framework, which was approved by the EU in 2000, is an important way for U.S. organizations to avoid interruptions in business dealings with the EU.

The U.S. Department of Commerce and the Federal Data Protection and Information Commissioner of Switzerland developed a separate "Safe Harbor" framework to bridge the differences in approach and provide a streamlined means for U.S. organizations to comply with Swiss data protection requirements. The U.S.-Swiss Safe Harbor Framework, which was approved in 2009, is an important way for U.S. organizations to avoid interruption in business dealings with Switzerland.

Self-certifying compliance with one or both of the Safe Harbor Frameworks assures European organizations that an organization provides adequate privacy protection, as defined by the relevant data protection law. From a U.S. perspective, the Safe Harbor program is a self-regulatory regime that is only available to organizations that are subject to the enforcement authority of the U.S. Federal Trade Commission or the U.S. Department of Transportation. Organizations that are outside of the jurisdiction of these two agencies are not eligible to join Safe Harbor.

Sensitive personal data / sensitive information – The EU Directive distinguishes between ordinary personal data, such as name, address, and telephone number, and sensitive personal data, defined as racial or ethnic origin, political opinions, religious beliefs, trade union membership, health, sex life, and criminal convictions. The processing of such data is prohibited unless specifically allowed by law. Special restrictions apply to the processing of such data.

***With the exception of those terms followed by the symbol ◊, the definitions for this Glossary were taken with the permission of the International Association of Privacy Professionals (IAPP), in whole or in part, from the IAPP Certified Information Privacy Professional Training Course Book**

https://www.privacyassociation.org/

U.S. Department of Commerce
U.S.-EU & U.S.-Swiss Safe Harbor Program
1401 Constitution Avenue, N.W.
Room 20007
Washington, DC 20230

E-mail: safe.harbor@trade.gov ▲ www.export.gov/safeharbor

March 2009* (Updated March 2013)