PRIVACY: THE U.S. “SAFE HARBORS”
to the
EUROPEAN UNION’S DIRECTIVE ON DATA PROTECTION

Introduction

On November 1, 2000, the “Safe Harbor” agreement between the European Union and the United States entered into effect. The agreement, which was ratified by the United States and the EU last summer, establishes a series of Safe Harbor Principles that will facilitate transfers of personal data from EU Member States to the United States that might otherwise violate provisions of the EU Directive on Data Protection. A U.S. organization that certifies compliance with the Safe Harbor Principles must voluntarily agree to a series of privacy protections in the United States for personal data received from the EU. The Principles protect, for example --

- An EU citizen’s right to “Notice” and “Choice” regarding the U.S. organization’s use and “Onward Transfer” of his or her personal data;
- “Access” by the EU citizen to personal data maintained by the U.S. organization; and
- “Enforcement” of the promised new protections through both dispute resolution mechanisms and sanctions imposed by a U.S. government agency such as the Federal Trade Commission.

As of November 1, 2000, virtually all U.S. organizations other than financial institutions are eligible to certify to the U.S. Department of Commerce their voluntary compliance with the Safe Harbor Principles.

There is, however, no immediate legal penalty for a U.S. organization that fails to certify. The EU has temporarily agreed to a “standstill” arrangement under which the enforcement provisions of the Directive will not be used to stop the flow of personal data to the United States, regardless of whether a U.S. organization receiving such data complies with the Safe Harbor Principles.\footnote{The standstill does not entirely eliminate the risk of legal sanctions arising from the Directive for the transfer of personal data from the EU to the United States because (1) the standstill is an informal commitment that an individual EU Member State could choose to ignore (which seems unlikely); and (2) it does nothing to prevent an individual in the EU from asserting a private right of action based on a violation of the Directive.} By mid-2001, EU and U.S. officials will make an initial assessment of whether the Safe Harbor Agreement is working, presumably based in part on the number of U.S. organizations that have chosen to certify. If there is agreement at that time to continue the Safe Harbor arrangement, the standstill likely would be lifted. A U.S. organization would then risk EU restrictions on personal data flows to the United States for failing to comply
with the Principles, unless it opted to rely on other provisions of the Directive that can be invoked to legitimize transfers of personal data to non-EU countries (e.g., contractual agreements and codes of conduct that provide the necessary privacy protections for transferred data, including enforcement mechanisms).

U.S. organizations that receive personal data from the EU will need to evaluate their circumstances very carefully to determine whether to certify voluntarily to the Safe Harbor Principles at this time. Department of Commerce officials have urged U.S. organizations to certify to reduce the risk that the EU will rescind its agreement to the Safe Harbor Principles. In that event, the EU could very well demand the imposition of even greater privacy restrictions on personal data flowing to the United States in order to find that the United States provides an “adequate” level of privacy protection. The Department of Commerce also asserts that, if the Safe Harbor Agreement is ultimately extended and the EU’s standstill is lifted, a U.S. organization that certifies will obtain clear legal certainty concerning its ability to transfer personal data to the United States without fear of EU sanctions. Moreover, an organization that certifies early may obtain a public relations benefit by advertising enhanced privacy protections to customers and employees.

Yet there are also costs to early Safe Harbor certification. By doing so, an organization makes broad public representations regarding enhanced privacy protections in the United States for the personal data of EU citizens. Such public representations directly increase exposure to legal liability in the United States for failure to abide by the promises made, a failure that would be subject to enforcement action by the Federal Trade Commission (or, in certain cases, the Department of Transportation). A U.S. organization that promises enhanced privacy protections to EU citizens alone (which is all that is required by the Principles) may also feel compelled as a practical and public relations matter to extend similar protections to personal data collected from individuals in the United States, thereby compounding its costs and legal exposure. Furthermore, an early certifier may incur the costs and increased legal exposure of certification without any guarantee that the Safe Harbor arrangement will in fact be permanent. And balanced against all these potential costs is the fact that an organization is very unlikely to suffer near-term legal consequences for failure to certify, so long as the standstill remains in place.

In deciding whether to certify to the Safe Harbor Principles, either now or in the future, an organization must also consider its alternatives for ensuring the uninterrupted flow of data from the EU. The Directive does permit certain transborder data transfers in limited circumstances, e.g., pursuant to contractual arrangements that provide adequate privacy protections to the EU data transferred. Yet such alternatives pose their own practical problems that may make them less attractive options than certifying to the Safe Harbor.

Whatever the option chosen, it is imperative that organizations begin the process now of assessing the best means for preserving the free flow of personal data from the EU to the United States.

Accordingly, this memorandum is intended to help organizations decide whether to certify their compliance with the Safe Harbor Principles. Part I summarizes the EU Directive on
Data Protection and its potential impact on the transfer of personal data from the EU to non-EU countries such as the United States. Part II is a more detailed description of the terms of the Safe Harbor Principles that would facilitate such transfers, and Part III provides practical advice regarding certain issues involved in Safe Harbor compliance. Part IV discusses alternatives to Safe Harbor certification. Finally, Part V discusses one final point related to compliance with the Directive in the EU.

Any questions about this memorandum, the Safe Harbor Principles, or the EU Directive on Data Protection may be directed to any of the lawyers listed below.

<table>
<thead>
<tr>
<th>Name</th>
<th>Location</th>
<th>Phone</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>John Dugan</td>
<td>Washington, DC</td>
<td>202-662-5415</td>
<td><a href="mailto:jdugan@cov.com">jdugan@cov.com</a></td>
</tr>
<tr>
<td>Richard Kingham</td>
<td>Washington, DC</td>
<td>202-662-5268</td>
<td><a href="mailto:rkingham@cov.com">rkingham@cov.com</a></td>
</tr>
<tr>
<td>Allison Cohen</td>
<td>Washington, DC</td>
<td>202-662-5666</td>
<td><a href="mailto:acohen@cov.com">acohen@cov.com</a></td>
</tr>
<tr>
<td>Erin Egan</td>
<td>Washington, DC</td>
<td>202-662-5145</td>
<td><a href="mailto:eegan@cov.com">eegan@cov.com</a></td>
</tr>
<tr>
<td>Louise Nash</td>
<td>London</td>
<td>20-7290-3124</td>
<td><a href="mailto:lnash@cov.com">lnash@cov.com</a></td>
</tr>
<tr>
<td>Kurt Wimmer</td>
<td>London</td>
<td>20-7290-3105</td>
<td><a href="mailto:kwimmer@cov.com">kwimmer@cov.com</a></td>
</tr>
<tr>
<td>Mark Kightlinger</td>
<td>Brussels</td>
<td>2-549-5248</td>
<td><a href="mailto:mkightlinger@cov.com">mkightlinger@cov.com</a></td>
</tr>
<tr>
<td>David Harfst</td>
<td>Brussels</td>
<td>2-549-5251</td>
<td><a href="mailto:dharfst@cov.com">dharfst@cov.com</a></td>
</tr>
</tbody>
</table>
# TABLE OF CONTENTS

## I. The EU Directive on Data Protection

A. Basic Principles of Data Protection
B. Rights of Individuals
C. Sensitive Data
D. Enforcement
E. Transfer of Personal Data

## II. Terms of the Safe Harbor Agreement

A. The Safe Harbor Certification Process
B. The Safe Harbor Principles
   1. Notice
   2. Choice
   3. Onward Transfer
   4. Security
   5. Data Integrity
   6. Access
   7. Enforcement
C. Limitations on the Application of the Principles
D. Additional Issues Addressed by FAQs
   1. Data Processing Contracts
   2. Human Resources Information
   3. Pharmaceutical and Medical Products

## III. Practical Issues Involved in Safe Harbor Compliance

## IV. Alternatives to the Safe Harbor

## V. Compliance in the EU: A Final Point
I. The EU Directive on Data Protection

The regulation of the use of personal data by EU Member States is nothing new. In the 1970s and 1980s, a number of European countries adopted privacy legislation. In 1980, the Organization for Economic Cooperation and Development (OECD) adopted guidelines on privacy protections and transborder data flows that were intended to lead to a coordinated approach. Because of the growing number of conflicts among Member State approaches to data protection, however, the EU perceived a need for greater harmonization of such legislation to facilitate free movement of personal data among Member States. Accordingly, in 1995 the European Parliament and the Council of the European Union adopted Directive 95/46/EC, otherwise known as the “Directive on Data Protection,” which establishes a set of uniform provisions governing the processing of personal data and the free movement of such data.

For the Directive to take effect in an EU Member State, that State must adopt implementing legislation. The Directive required all EU Member States to enact such legislation by October 25, 1998, and to date Austria, Belgium, Denmark, Finland, Greece, Italy, the Netherlands, Portugal, Spain, Sweden, and the United Kingdom have done so.\footnote{The remaining Member States (France, Germany, Ireland, Luxembourg) have yet to pass implementing legislation (although most of these countries already had in place a comprehensive privacy law that pre-dated the Directive). The European Commission has initiated proceedings to compel several Member States to implement the Directive.}

In general, the Directive places obligations on “data controllers” with respect to the use of personally identifiable data. (“Data controller” means a natural or legal person that determines the purposes and means of processing of personal data.) The Directive applies to data controllers that are established in the EU and process personal data in the context of their EU activities. It also applies to data controllers that, while not established in the EU, use equipment situated in the EU to process personal data.\footnote{There is a strong argument that the Directive does not apply where a non-EU data controller’s only contact with an individual in the EU is through an Internet website, so long as the website server is also located outside the EU. Nevertheless, there is no definitive precedent on this issue, and some commentators (including some Department of Commerce staff) have suggested that the Directive does in fact apply to such website data collection and transfer. The Safe Harbor Agreement does nothing to resolve this issue. In the official exchange of letters establishing the Agreement, Department of Commerce and EU officials expressly stated that their discussions “have not resolved nor prejudged the questions of jurisdiction or applicable law with respect to websites.”} The Directive applies both to personal data processed by computer or other automatic means and to data held manually in a filing system (such as card indexes, microfiches, and paper files about individuals).

Under the Directive, in addition to registering its processing activities with a national supervisory body, a data controller must comply with basic principles of data protection that
regulate the manner in which personal data may be collected, held, and processed. The Directive also specifies the rights that individuals have with respect to such personal data held by others; establishes special obligations for “sensitive” information; includes specific provisions regarding enforcement; and imposes significant restrictions regarding the transfer of personal data to non-EU countries. Each of these aspects of the Directive is briefly discussed below.

A. Basic Principles of Data Protection

- **Fair and Lawful Processing:** Personal data must be processed fairly and lawfully.

- **Purpose:** Personal data may only be collected for specified, explicit, and legitimate purposes, and may not be further processed in a way that is incompatible with those purposes.

- **Relevance:** Personal data collected must be adequate, relevant, and not excessive in relation to the purposes for which they are processed.

- **Accuracy:** Personal data must be accurate and, where necessary, kept up to date.

- **Retention:** Personal data must not be kept in a form that permits identification of individuals for longer than is necessary.

- **Security:** Data controllers must implement appropriate security measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure, or access.

B. Rights of Individuals

The Directive provides individuals with certain rights with respect to data that are held about them, including the following:

- **Right to object to use of data for marketing purposes:** An individual has an express right to object at any time to his or her data being used for direct marketing purposes.

- **Access:** An individual has a right of access to his or her personal data held by a data controller. That is, in response to an individual’s request, a data controller must describe, among other things, the categories of personal data held; the purposes for which the data are held; and the categories of recipients to whom the data are disclosed.

- **Rectification, Erasure and Blocking:** An individual has a right to require the data controller to rectify, erase, or block any data that are incomplete or inaccurate.
C. Sensitive Data

Additional restrictions apply to the processing of “sensitive” data, i.e., data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, or sex life. In most circumstances, it is necessary to obtain the explicit consent of an individual to process data that fall within this category.

D. Enforcement

Member States have broad discretion to adopt suitable measures to enforce the requirements of the Directive. These measures vary from Member State to Member State, but typically include rights for the national supervisory authority for data protection to investigate alleged infringements of legislation that implements the Directive. Significantly, the Directive also requires the establishment of a private right of action for an individual who has suffered damage as a result of an infringement of privacy legislation implementing the Directive. Specifically, the individual must be entitled to receive compensation from the entity processing his or her data for the damage suffered.

E. Transfer of Personal Data

As described above, any organization that collects and processes personal data in an EU country will have to comply with the significant level of privacy restrictions that arise from that country’s legislation that implements the terms of the Directive. A further issue arises, however, when such an organization seeks to transfer such personal data from the EU country, where they are subject to the Directive’s protections, to a non-EU country, where they are not. The Directive squarely addresses this issue by tightly restricting such transfers.

Under Article 25 of the Directive, the general rule is that personal data can only be transferred outside the EU when the data will receive “adequate” protection in the country to which the data are transferred. The term “adequate” is not defined, and the Directive provides the European Commission with significant latitude to make an “adequacy” determination regarding the level of privacy protection afforded by an importing country in light of all the circumstances surrounding the transfer. Specifically, the Commission can rule that particular non-EU countries provide adequate protection, permitting free movement of data to such countries.

The Directive contains a number of important exceptions to the general rule that personal data may only be transferred to non-EU countries that satisfy the “adequacy” standard. For example, the general rule does not apply where an individual has given unambiguous consent to the transfer, or where the transfer is necessary for the performance of contractual obligations to the individual (although the latter exception has been interpreted quite narrowly).

Importantly, as discussed in more detail below, personal data may also be transferred to a non-EU country where adequate safeguards are implemented through contract. For example, a company in the EU that wishes to transfer data to a company located outside the EU could
enter into a contract with the importing company under which the latter would promise to provide adequate safeguards to the data transferred.

II. Terms of the Safe Harbor Agreement

EU officials have taken the position that the United States’ existing patchwork of sectoral privacy laws does not provide an “adequate” level of privacy protection to personal data transferred from the EU to the United States. The Safe Harbor Agreement provides a mechanism that has allowed the European Commission to determine that the United States may provide “adequate” protection to personal information transferred from the EU to U.S. organizations -- but only where the recipient U.S. organization complies with the Safe Harbor Principles summarized below.

A. The Safe Harbor Certification Process

A U.S. organization may qualify for the Safe Harbor in different ways: (1) it may join a self-regulatory privacy program that requires its members to adhere to the Safe Harbor Principles; (2) it may develop its own self-regulatory privacy policies; or (3) it may follow a body of law or rules that effectively protects personal privacy. An organization that relies in whole or in part on self-regulation to implement the Safe Harbor Principles must be subject to the enforcement jurisdiction of either the Federal Trade Commission (FTC) or the Department of Transportation (DOT) for failure to abide by the Principles. (These two agencies have jurisdiction over virtually all U.S. organizations other than financial institutions.)

To claim Safe Harbor status, a U.S. organization must “self-certify” to the Commerce Department its adherence to the Safe Harbor Principles. This certification occurs by providing the Department with an annual letter (by mail or through Internet certification) that contains the name of the organization and its contact information, a description of the activities of the organization with respect to personal information received from the EU, and a description of the organization’s privacy policy for such personal information. The privacy policy description must include, among other things, (1) where the policy is available for public viewing, and (2) certain required disclosures relating to how the organization adheres to the requirements of the Safe Harbor Agreement (e.g., the name of any privacy programs in which the organization is a member, the organization’s method of verifying compliance with the Safe Harbor Principles, and the independent recourse mechanism that is available to investigate unresolved complaints).

B. The Safe Harbor Principles

The Safe Harbor Agreement sets forth seven Safe Harbor Principles: Notice, Choice, Onward Transfer, Security, Data Integrity, Access, and Enforcement. The Agreement also

---

4 Financial institutions are subject to new federal financial privacy regulations that may lead to a separate “adequacy” determination, depending on the outcome of ongoing negotiations between the U.S. Treasury Department and the European Commission.
includes 15 Frequently Asked Questions (FAQs), which address specific interpretive issues raised by the Principles. Set forth below are each of the seven Principles, with selected comments.

1. 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.

Comment: Notice is not required for disclosures made to a third party that is acting as an agent to perform a task on behalf of and under the instructions of the U.S. organization. (However, the Onward Transfer Principle applies to such transfers.) In addition, the Notice, Choice, and Onward Transfer Principles generally do not apply to public record or publicly available information so long as it is not combined with non-public record information.

A U.S. organization is not required to provide separate or additional notice if adequate notice was provided to the individual in the EU when the data were collected. That is, an organization in an EU Member State that collects personal data from an individual in the EU must comply with the notice requirements of the Directive, as implemented by that Member State. If the organization then transfers that data to a U.S.-based organization that complies with the Safe Harbor Principles, and that transfer is consistent with the notice given to the individual in the EU, then the Safe Harbor Principles would not require the U.S. organization to provide any additional notice to that individual.

2. 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 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 data any information received from a third party where the third party treats and identifies it as sensitive.

Comment: Opt-out choice must be provided when non-sensitive personal information is provided to a “third party,” a term that includes both unaffiliated companies and companies affiliated by common ownership (such as another subsidiary owned by the same parent company). Opt-out choice must also be provided for the U.S. organization to use personal information for any purpose that is “incompatible” with the purpose for which it was collected. This seems to suggest that, as long as a purpose for collecting information has been disclosed to an individual, it is not necessary to provide opt-out choice in order for the U.S. organization to use the information for that purpose. However, FAQ 12 provides that a company should give an individual an opportunity to opt out of having personal information used for direct marketing at any time, even if such marketing was disclosed to the individual at the time the data were collected.

With respect to the opt-in requirement for the disclosure or use of sensitive data, exceptions apply, e.g., to establish legal claims or defenses; to provide medical care; and to carry out employment law obligations.

As with the Notice principle, it is not necessary to provide either opt-out or opt-in choice when disclosure is made to a third party that is acting as an agent to perform a task on behalf of and under the instructions of the U.S. organization (subject to the Onward Transfer principle). There are no other exceptions to the Choice principle for use and third-party transfer (other than the general limitations on the application of all the principles, discussed below).

3. 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, 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.

Comment: It appears likely that most organizations would comply with this requirement through standard contractual arrangements with third parties that strictly limit their use and onward transfer of personal information.
4. 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.

Comment: The Security principle applies to how a U.S. organization stores, processes, maintains, and protects personal data of an EU citizen that are transferred from the EU to the United States. An organization should take steps to secure such personally identifiable information in addition to (and in accordance with) its privacy policy, e.g., by securing its computer systems and/or paper files.

5. 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.

Comment: By limiting collection to relevant information only, the Data Integrity principle minimizes the risk that personal information would be misused or abused by a U.S. organization. Compliance with this principle is also intended to decrease the risk that an organization’s decisions would be based on erroneous or inappropriate information.

6. 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.

Comment: The right of access to personal data is not absolute, but is instead subject to the limits of proportionality and reasonableness. For example, a company may consider factors such as the burden and expense of providing access, and the importance of the information requested, in determining whether a request is reasonable. In addition, a company is not required to provide access to its data bases or to restructure its data bases to be able to provide access. And a company may deny access in a number of specifically defined circumstances, such as where the disclosure is of personal information that is processed solely for research or statistical purposes; where the disclosure would interfere with law enforcement or private causes of action; or where it would prejudice employee security investigations or grievance proceedings.
Significantly, FAQ 8 indicates that access may be required to some forms of derived personal data, such as non-sensitive marketing data that are used to determine whether or not to send an individual a catalog. On the other hand, access is not required to “confidential commercial information,” a term taken from the U.S. Federal Rules of Civil Procedure that refers to information that an organization “has taken steps to protect from disclosure, where disclosure would help a competitor in the market.” The FAQ further states that “a computer program, modeling program, or the details of that program may be confidential commercial information,” and that an organization may deny or limit access to avoid revealing its own confidential commercial information, “such as marketing inferences or classifications generated by the organization.” This language appears to shield from access proprietary “profiling” information, which may be of critical concern to many organizations that are considering whether to certify to the Safe Harbor Principles.

7. Enforcement

Effective privacy protection must include mechanisms for assuring compliance with the Principles, recourse for the 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.

Comment: An organization can meet the “independent recourse mechanism” and “remedy” requirements of the Enforcement principle in one of three ways: by complying with a private sector privacy program that enforces the Safe Harbor Principles; by complying with a legal or regulatory supervisory authority that handles individual complaints and dispute resolution; or by committing to cooperate with the Data Protection Authorities located in the EU. The “verification” requirement can be satisfied through self-assessment or outside compliance reviews.

It should be emphasized that it will not be sufficient under the Enforcement principle for a U.S. organization merely to self-certify; adopt a privacy policy; and subject itself to potential FTC enforcement for failure to abide by that privacy policy (which the FTC would regard as an unfair or deceptive act or practice under section 5 of the Federal Trade Commission Act). More is required; that is, the independent recourse mechanism will also require a U.S. organization to submit to potential sanctions from a third party (e.g., a privacy self-regulatory organizations (SRO) or an EU Data Protection Authority) arising from an individual’s complaints about the organization’s failure to abide by the Safe Harbor Principles.
The FTC has also committed to review on a priority basis referrals received from such a third party alleging non-compliance with the Safe Harbor Principles. Again, the source of the FTC’s legal authority is its ability to find that a violation cited by an SRO or EU Data Protection Authority constitutes a failure of the organization to comply with the Safe Harbor framework. Such a failure to comply may be deemed by the FTC to constitute an unfair or deceptive practice in violation of the FTC Act. If the FTC has reason to believe that such a violation has occurred, it may seek an administrative cease and desist order prohibiting the challenged practices, or it may file a complaint in a federal district court, which, if successful, could result in a court order to the same effect. A U.S. organization that does not comply with an FTC order may be subject to a court-imposed civil penalty of up to $12,000 per day (per violation).

Unlike the Directive, the Enforcement principle does not establish a private right of action for individuals as a matter of federal U.S. law. Nevertheless, U.S. companies have expressed concern about the possibility of private rights of action arising under those U.S. state laws that, like the FTC Act, prohibit “unfair or deceptive practices” (so-called “mini-FTC Acts”), but, unlike the FTC Act, have express private rights of action.

The Safe Harbor Principles and the FAQs will be enforced in the United States. U.S. law will apply to questions of interpretation and compliance with the Principles, FAQs, and relevant privacy policies, except where a U.S. organization has committed to cooperate with a Data Protection Authority in order to satisfy the “independent recourse mechanism” requirement.

C. Limitations on the Application of the Principles

The Safe Harbor Preamble recognizes three general limitations on the application of the Principles. First, adherence to the Principles may be limited to the extent necessary to meet public interest requirements, such as health and safety, as well as national security or law enforcement requirements. Second, the Principles may not apply when U.S. law creates conflicting obligations or explicit authorizations. Third, application of the Principles may be limited when exceptions are permitted by the Directive or by Member State law, such as where a transfer of personal data is necessary to satisfy a contractual obligation owed by the transferor to an individual.

D. Additional Issues Addressed by FAQs

The FAQs address additional issues that are relevant to the Safe Harbor Agreement. Three of these issues -- the effect of data processing contracts, the transfer of human resources information, and the treatment of data developed in pharmaceutical or medical research – are discussed below.

1. Data Processing Contracts

Article 17 of the Directive requires a European data controller to enter into a contract when it transfers data for processing purposes, whether the processing operation occurs inside or
outside the EU. When data are transferred from the EU to the United States, Article 17 applies, regardless of participation by the U.S. processor in the Safe Harbor. A U.S. company participating in the Safe Harbor and receiving personal information from the EU merely for processing does not have to apply the Safe Harbor Principles to this data.

2. Human Resources Information

The Safe Harbor covers the transfer of personal information about an employee from an EU company to a parent, affiliate, or unaffiliated service provider in the United States. This transfer is subject to any conditions and restrictions imposed by the national laws of the EU country where the information was collected and processed. A U.S. organization need not provide Notice and Choice to an individual if it intends to use his or her employee information solely in the context of an employment relationship. On the other hand, if an organization plans to disclose such information to a third party and/or use it for non-employment related purposes, it must do so in accordance with the Notice and Choice principles.

3. Pharmaceutical and Medical Products

The Safe Harbor Principles apply to personal data developed in pharmaceutical or medical research once they are transferred to a U.S. organization. They do not, however, cover personal data that are uniquely key-coded so as not to reveal the identity of individuals. The Safe Harbor addresses the treatment of clinical data in a number of situations, including their use in new scientific research; their continued use after the voluntary withdrawal of an individual from a clinical trial; their submittal for regulatory purposes; access to them in “blinded” studies; and the application of certain Safe Harbor Principles to them for regulatory reporting.

III. Practical Issues Involved in Safe Harbor Compliance

In deciding whether to comply with the Safe Harbor Principles, organizations will need to consider the practical consequences of compliance, including, among others, the following:

- **Separate Rules for EU Citizens?** The Safe Harbor Principles apply only to the personal data of EU citizens collected in the EU and transferred to the United States. As a result, it is only necessary to provide the enhanced privacy protections of the Safe Harbor to such data, and there is no requirement to provide those protections to the personal data of U.S. citizens collected in the United States. If an organization plans to apply the Safe Harbor Principles only to personal data received from EU citizens, it must decide how to segregate or “tag” the data for separate treatment, and it will need to assess whether the systems, compliance, and training issues raised by such dual tracking can be resolved in a practical manner. The organization must also decide whether, as a public relations or customer service matter, it is defensible to establish greater privacy protections for EU customers or employees than for those in the United States. If an organization is considering the adoption of Safe Harbor-like protections for all of its U.S. customers and employees, it should carefully assess the increased costs and legal exposure of doing so.
• **Privacy Policy.** To demonstrate compliance with the Principles, an organization must adopt a publicly available privacy policy that conforms with the terms of the Principles with respect to personal data received from the EU, *i.e.*, one that describes the organization’s method of adhering to the Safe Harbor Principles of Notice, Choice, Access, Enforcement, etc. An organization that makes such public promises will have to abide by them or risk the enforcement actions contemplated by the Principles.

• **Privacy Notices.** A U.S. organization may need to prepare a special privacy notice for EU citizens whose information is transferred from the EU to the United States. This would be required if the organization intends to use or disclose such personal information in a manner that is inconsistent with any notice previously provided under the Directive to such individuals in the EU when the information was collected. Such notices must be clear and conspicuous and may simply reiterate the terms of the privacy policy described above.

• **Corporate Privacy Staff.** Irrespective of size, an organization should designate staff to oversee compliance with the organization’s privacy policy (including any separate privacy policy adopted for the data of EU citizens). In large organizations, a centralized approach will increase the likelihood that the policy is consistently applied throughout the organization and minimize the risks of non-compliance.

• **Training.** Staff education and awareness are key to ensuring compliance with the organization’s privacy policy and procedures. Once such procedures have been adopted, a high-profile organization can expect them to be tested by interested parties, such as journalists. An organization must educate its staff about the importance of ensuring that the organization’s privacy practices comply with its privacy policy. This could be achieved through training courses (both general courses and course targeted to specific areas of the business, *e.g.*, marketing or sales), regular awareness bulletins, or the use of privacy software training packages.

• **Security.** Organizations must implement security systems to protect personal information. Such systems might include physical entry controls, secure computer rooms and data centers with restricted access, measures to protect against viruses, and access control procedures, such as the cancellation of rights of access when staff members leave or change divisions within an organization.

• **Access.** Organizations must implement systems for dealing with requests from individuals to access their information. This might involve preparing standard access request forms and forms of response for follow-up inquiries and final responses.

• **Enforcement.** Certification under the Safe Harbor Principles increases exposure of U.S. organizations to U.S. legal sanctions.

  - Any public representations made in the United States by adopting or changing the terms of a privacy policy, or by otherwise promising to abide by the Safe Harbor Principles, exposes an organization to FTC
enforcement sanctions for any subsequent failure to abide by such representations.

- Such a failure may also expose the organization to U.S. state law sanctions on similar grounds, including private rights of action.

- In addition, the “independent recourse requirement” may lead to legal exposure. An organization that agrees to join a privacy self regulatory organization (SRO) must bind itself to the results of the individual dispute resolution mechanisms of that SRO (or face enforcement sanctions from the FTC for failure to abide by the Safe Harbor Principles). For example, depending on the type of dispute resolution mechanism adopted by a particular SRO, potential sanctions could include publication of findings of non-compliance; required deletion of data; compensation to individuals for losses incurred as a result of non-compliance; injunctive orders; and suspension or removal of a “seal of approval” (which could have a negative impact on customer relations). Moreover, an SRO’s referrals of violators to the FTC may make it more likely that the FTC would take an enforcement action than might otherwise be the case.

- One Internet privacy seal program, TRUSTe, has already announced that it will provide a Safe Harbor privacy program that will include website certification, oversight, and dispute resolution, and it is expected that other privacy organizations will soon make similar programs available.

- **Verification Measures.** Organizations must establish follow-up mechanisms to ensure that statements made about Safe Harbor privacy practices are accurate. Such verification can either be achieved by means of self-assessment or outside compliance reviews. If an organization elects to adopt the self-assessment approach it should, at a minimum, carry out annual audits to determine whether:

  - The organization’s privacy policy is accurate, comprehensive, prominently displayed, completely implemented, and accessible.

  - The privacy policy conforms to the Safe Harbor Principles.

  - Individuals are informed of any in-house arrangements for handling complaints and of the independent mechanisms through which they can pursue complaints.

  - The organization has adopted procedures for training employees in the implementation of the privacy policy and disciplining them for failing to follow it.

  - The organization has in place internal procedures for periodically conducting objective compliance reviews.
To assist with any internal audit, organizations might seek guidance from external consulting firms and advisers, as well as from materials issued by the various EU Data Protection Authorities. Internal audits might, among other things, include the identification of new forms of processing and verification that all new staff members have received appropriate training and that any access requests or complaints have been recorded and handled appropriately.

IV. Alternatives to the Safe Harbor

Rather than certify to the Safe Harbor Principles, organizations may choose other methods for transferring data from the EU to the United States (or to any other country that has not received an “adequacy” determination from the European Commission). The Directive provides essentially four alternatives to participating in the Safe Harbor:

- **Consent.** An organization may decide to obtain the consent of each individual whose data it transfers. The individual’s consent must be unambiguous. In some circumstances, consent may be implied from the individual’s decision to provide personal information. However, in many circumstances, particularly if “sensitive” data are being transferred, express consent will be required. This approach does not provide the same degree of legal certainty as the Safe Harbor, because organizations that rely on it may be vulnerable to attack from individuals or Data Protection Authorities on the basis that the consent was not “unambiguous”; that the consent was not fully informed; or that the data had been processed for a purpose to which the individual had not consented. Any such determination would obviously undermine all transfers made in reliance on this approach. In addition, organizations relying on this approach would need to maintain permanent and reliable records of consents obtained.

- **Special Exemptions.** Organizations could seek to rely on one or more of the Directive’s specific exemptions from the restriction on transfer. These include where the transfer is necessary (1) for the performance of a contract between the individual and the organization; (2) on public interest grounds or for the establishment, exercise, or defense of legal claims; or (3) for the individual’s vital interests. Reliance on these exemptions will require an analysis of all relevant circumstances of each individual transfer and is therefore unlikely to be appropriate unless all or a significant number of transfers made by an organization are of a particular category that falls within one of the exemptions.

- **Inter-company agreements.** An organization could also adopt a contractual solution to the issue of information transfers. This would involve the transferring company contracting with the companies to which it transfers data (whether part of the same group or third parties) on terms that require each receiving company to process personal information originating from the EU in accordance with a set of strict conditions designed to safeguard those data. Those conditions would likely need to be as stringent as the terms of the Safe Harbor, as that is likely to be viewed as the minimum level of acceptable protection by the EU authorities. But, unlike the certification contemplated by the Safe Harbor Agreement, any such contractual conditions would not likely be subject to the enforcement jurisdiction of the United States.
The form of contract could be prepared by the organization in question based on model clauses prepared by an industry association such as the International Chamber of Commerce (ICC). It should be noted that, at present, the contractual approach to compliance is regarded as having a number of shortcomings, not least of which is the possible lack of direct enforceability of the contract by the individual. These issues have meant that, as yet, no set of model contract clauses has been approved by the European Commission. Unless and until a set of model clauses has been endorsed by the Commission, organizations will face a degree of uncertainty as to the effectiveness of any contractual solution they might adopt.

**Codes of Conduct.** An organization could, alternatively, adopt a code of conduct as a framework for the way in which personal data are processed by, and across, the organization. The simplest method to do this would be for the organization to prepare a code for internal use. A more costly and time-consuming approach would be to prepare a code for application across its particular industrial sector as a whole.

The Directive encourages the use of codes of conduct to contribute to the proper implementation of that legislation and makes specific reference to the preparation of codes by trade associations. If an organization wants a degree of certainty that its code provides an acceptable level of protection, it can seek a formal ruling from the European Commission that the code is consistent with the Directive. Obviously, seeking a formal ruling would prolong the overall process involved in finalizing a code, as protracted negotiations with the European Commission would inevitably result. Further, it is not yet clear whether an individual corporation would be able to take advantage of the process for seeking the Commission’s ruling on any code it adopted or whether the procedure is intended only for industry associations. As with the contractual solution, a code of conduct would need to be rigorously enforced throughout the organization to be considered credible.

V. **Compliance in the EU: A Final Point**

This memorandum focuses principally on the transfer of personal information from the EU to the United States (and elsewhere). However, it is important to remember that organizations with a presence in one or more EU Member States must comply with Member State law that implements the Directive. Although the fundamental principles underlying such implementing legislation will be the same in different Member States, there is and will be no uniformity of data protection law across the EU.

Thus, depending on the number of Member States in which an organization operates, the organization may find itself subject to the laws of several Member States simultaneously. However, an organization may be able to avoid such a result by restructuring its operations so that it is subject only to one Member State’s law.