00-214

December 1, 2000

To: EEAC Members

From: Jeffrey A. Norris
President

Re: **EU Data Protection Directive Update: U.S. Commerce Department Posts "Safe Harbor Workbook" To Help Employers Understand Compliance Obligations**

The U.S. Department of Commerce (DOC) has posted on its website additional information designed to help multinational companies understand their obligations with respect to cross-border transmission of "individually identifiable" employee information under the controversial European Union (EU) Data Protection Directive. DOC's most recent posting contains a "Safe Harbor Workbook," which provides a step-by-step explanation of the Safe Harbor Principles negotiated between Commerce and the European Union that permit companies to self-certify that they provide "adequate" privacy protection in compliance with the Directive.

The EU Data Protection Directive severely restricts the flow of personal data out of any of the 15 EU member countries. The Safe Harbor Principles agreed to by DOC and EU negotiators earlier this year provides U.S. companies who do business in the EU with a means of some assurance that data flow from the EU to the U.S. will not be interrupted. In addition to the Workbook, DOC also has posted a self-certification form and checklist. The Workbook encourages U.S. companies that receive individually identifiable information from the EU to consider self-certifying to the Principles if they have not yet found some other way to demonstrate "adequacy" or some exception in the Directive that excuses noncompliance.

Attached for your information is a copy of DOC's Safe Harbor Workbook (Attachment 1). It also can be found online at *http://www.export.gov/safeharbor/SafeHarborWorkbook.htm*.

The EU Data Protection Directive

The EU was organized in the late 1960's as part of a post-World War II effort by European countries to cooperate economically and socially. Today, 15 countries are members of the EU: Austria, Belgium, Denmark, Finland, France, Germany, Greece, Ireland, Italy, Luxembourg, The Netherlands, Portugal, Spain, Sweden, and the United Kingdom. EU

Directives have the force of law for all of the EU member countries. In addition, each member country is required to pass its own legislation incorporating the requirements of any EU Directive.

The Data Protection Directive, which can be found on the internet at *http://europa.eu.int/eur-lex/en/lif/dat/1995/en_395L0046.html*, took effect in October 1998, but enforcement was delayed pending negotiations between the U.S. government and EU authorities on how U.S. multinationals would be able to comply. The Directive imposes significant requirements on companies who process "personal data" that can be identified directly or indirectly to an individual. It also places severe restrictions on the transmission of personal data outside the EU. Member countries must stop the transmission of such data, according to the Directive, if the receiving country lacks adequate privacy safeguards, subject to some limited exceptions. For additional information on the Directive, see EEAC Memorandum 98-203 (November 25, 1998).

The Safe Harbor Principles

In the EU's view, the U.S. lacks adequate privacy safeguards. For this reason, an EU member country can stop the flow of data from, for example, a foreign subsidiary to its U.S. parent if the two companies do not have procedures in place that meet the Directive's adequacy requirements.

In an effort to provide a workable solution, the U.S. Department of Commerce negotiated with the EU a set of "Safe Harbor Principles." See EEAC Memorandum 00-145 (August 18, 2000). The Principles are designed so that if a U.S. company adheres to them, it will meet the adequacy requirements for transfer of individually identifiable information outside of the EU. The text of the Safe Harbor Principles follows:

- **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.

- **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 defined "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, 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

[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.

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.

  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.

Self-Certification

Implementation of the Principles is by means of a voluntary self-certification process that went into effect on November 1, 2000, and which is administered by DOC. See EEAC Memorandum 00-170 (September 22, 2000). If a company wants to take advantage of the safe harbor, it must meet all of DOC's requirements for self-certifying that it is adhering to the Safe Harbor Principles, including:

- initial registration by a corporate officer;

- annual self-certification to the DOC that the company abides by the safe harbor requirements;

- adoption of a privacy policy addressing each of the seven privacy principles and the relevant points in frequently asked questions on DOC's website that further explain the Principles;

- adoption of procedures to verify compliance;

- implementation of an effective dispute resolution system to investigate, resolve and remedy individual complaints;

- a commitment to cooperate with the EU data protection authorities and to take their advice (*mandatory only if the company is electing to adhere to the Principles for the purpose of transferring human resources information*); and

- enforcement by the Federal Trade Commission or other applicable federal agency.

DOC maintains a "safe harbor list" of companies that have self-certified and posts it on its website at *http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+list*. As of this writing, only three companies are listed: the Dun & Bradstreet Corporation, a search firm for privacy executives, and a firm that provides privacy resources for web publishers.

DOC's Safe Harbor Certification Forms and Workbook

As of November 1, 2000, companies wishing to take advantage of the safe harbor must self-certify to DOC by letter or online. DOC recently added to its safe harbor website an online self-certification form (Attachment 2) as well as "Certification Information" providing a list of required information for companies to review before actually completing the certification form (Attachment 3).

The DOC's Safe Harbor Workbook (Attachment 1) offers additional guidance on each step of the self-certification process. The Workbook outlines the required contents of a company's privacy policy, stating that "the policy must address the seven privacy principles and any relevant points that are covered in the frequently asked questions (FAQs), reflect your actual and anticipated information handling practices, and clearly state that you are in compliance with the safe harbor privacy principles". The Workbook then provides the DOC's commentary on each of the Principles as applied to a company privacy policy. It does not supply form language.

Special Considerations for HR Data

Since the Safe Harbor Principles apply to all uses of personal data, the Workbook itself is not geared towards human resources data. Several of the FAQs, however, do address HR data. FAQ 9 is entitled "Human Resources" and outlines the applicability of the Principles to HR data. FAQ 6, which sets out the requirements for self-certification, includes additional requirements that apply when a company wants to transfer HR data. FAQ 5, which addresses the role of the data protection authorities (DPAs) in each EU member country, also is relevant, since FAQ 9 requires companies to commit to cooperate with the DPAs if they are transferring HR data. These FAQs are attached to EEAC Memorandum 00-170 and also are posted on the DOC's website. Of the three companies listed to date on DOC's safe harbor list, only one has self-certified with respect to HR data.

Practical Considerations Concerning Self-Certification

According to the DOC Workbook, a company that self-certifies that it is adhering to the Safe Harbor Principles gains the benefit of "predictability and continuity" of uninterrupted data transfers from the EU. Unless a company "persistently fails to comply" with the Principles, a company that annually self-certifies will enjoy the security of the safe harbor.

At the same time, EEAC is aware that some companies have indicated concerns about the commitments they would be making if they elect to self-certify compliance with the safe harbor.

First, as noted above, FAQ 9 requires companies who wish to transfer HR data to "commit to cooperate in investigations by and to comply with the advice of" the EU data protection authorities, a rather broad concession.

Second, in addition to voluntarily submitting to the jurisdiction of the DPAs, a company also places itself under the jurisdiction of the U.S. Federal Trade Commission (FTC). According to FAQ 5, "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 [Federal Trade Commission] Act or other similar statute." This section, 14 U.S.C. § 45, enables the FTC to sue a violator and obtain an injunction as well as a penalty of up to $10,000 for each violation.

Third, the privacy protections offered by the safe harbor's required privacy policy are considerably broader than many companies are likely to want to extend to their U.S. employees. There may be other issues as well.

Other Strategies To Comply With the EU Data Protection Directive

Some companies are looking at other options besides adherence to the Safe Harbor Principles as a means of complying with the EU Data Protection Directive. It is our understanding, however, that no single best compliance option has emerged to date.

One possibility is adoption of a policy not to transfer individually identifiable information to the U.S., and to send HR data only in the aggregate. This option may be extremely difficult in practice, however. First, the U.S. company may have a need for personal data. Second, a total prohibition may be virtually impossible to monitor, bearing in mind that a single e-mail from an EU location to the U.S. with an employee's name could give rise to a violation.

A second option involves attempting to take advantage of one of the exceptions contained in Article 26 of the EU Directive. For example, Article 26 provides that a transfer of personal data may take place if "the data subject has given his consent unambiguously to the proposed transfer." Some companies are considering whether it would be feasible to obtain consent from their employees prior to making the transfer. Again, this option may be easier said than done.

Yet another option involves creating a contract between the EU company and the U.S. company in which the U.S. company agrees to abide by the EU Data Protection Directive. We understand, however, that such a contract would require approval by the data protection authorities in each country involved. Although at least one organization representing international businesses has drafted model language, we are not aware that it has been accepted by the DPAs.

Further Developments

As EEAC has been reporting over the last two years, the implementation of the EU's Data Protection Directive and the adoption of the Safe Harbor Principles have significant implications for U.S. companies that obtain data from affiliates operating within the EU. Our focus, of course, has been on the aspects of the Directive and Principles that impact the cross-border transmission of HR data. Having said that, we do not pretend to be experts on EU procedures or requirements, nor do we have the answers as to the best way to approach compliance. Accordingly, we strongly recommend that potentially affected member companies consult with internal counsel as how to best proceed.

In the meantime, EEAC will continue to monitor and report on further developments, including any additional guidance that may be issued, as they occur.

Questions concerning this memorandum may be addressed to Ann Elizabeth Reesman at 202-789-8650.