SAFE HARBOR, PRIVACY, AND HUMAN RESOURCE DATA MANAGEMENT

Stephen Hogan, Southeastern Oklahoma State University
C. W. Von Bergen, Southeastern Oklahoma State University

ABSTRACT

Recently the United States (US) Department of Commerce and the European Commission, the executive branch of the European Union (EU), reached an agreement on data privacy for information on citizens being transferred between the United States and the European Union. US companies that certify to the Department of Commerce that they are complying with the principles of the Safe Harbor Agreement are assured no interruption in data transfers between the US and the EU. Implications of this agreement for human resource managers are discussed.

I. INTRODUCTION

Effective October 1, 2000 the US Department of Commerce officially agreed with the European Commission, the executive arm of the EU, to require the EU's data privacy policy in the US. This agreement, known as the Safe Harbor Agreement, commits the US government as guarantor of the privacy of EU citizens whose personal data are transmitted to US businesses and other organizations (US Department of Commerce, 2000).

The Agreement has far-reaching implications for *all* US organizations and their human resource operations, not just those with dealings in Europe. If the Agreement withstands constitutional scrutiny, it will compel human resource managers to alter how they use employee data and to treat them with far more privacy than previously may have been the case.

II. US AND EU VIEWS ON PRIVACY

How much privacy protection nations offer varies with how open their societies are. By common assent, for instance, the US has one of the more open societies in the world, with personal privacy and the privacy of personal information not especially pressing concerns until only relatively recently. Because of this cultural openness there is not much history in US common law and legislation on data privacy.

While the US has long recognized a right to privacy in certain actions, it has not typically recognized a *fundamental* right to privacy of personal data. Rather, the traditional view is that data are a commodity that can be freely bought and sold. According to this view, a business need not pay consumers to obtain or use data about them, and a business can generally sell those data without legal hindrance to anyone it chooses although this seems to be changing because of the litigation involving bankrupt firms ToysMart.com and APB Online.

The US has generally favored an approach toward data privacy which relies on a mixture of self-regulation, government regulation, and legislation. Where legal limitations do exist, they are not comprehensive in nature, but are rather patchwork in scope and relate only to specific instances of privacy. To illustrate, the Video Privacy Protection Act prohibits disclosure of personal data gathered through video rentals; the Fair Credit Reporting Act limits how certain financial data can be used and shared; and the just-enacted Electronic Signatures Act recognizes digital signatures as equivalent to traditional (and highly private) personal signatures.

European society, on the other hand, appears less open and far less tolerant of easy access to private personal information. The EU elevates individuals' rights to personal data protection as a fundamental right–the right to privacy–and this view has found formal expression in virtually all major Western Europe agreements. Europe's initial expression of this, for example, and one its war-torn societies insisted upon, came in the United Nations' Universal Declaration of Human Rights in 1948, declaring for the first time that "no one shall be subjected to arbitrary interference with his privacy...or correspondence...Everyone has the right to the protection of the law against such interference or attacks." Similar language also appeared in the European Convention for the Protection of Human Rights and Fundamental Freedoms in 1950 and the Treaty of Rome in 1957 establishing the European Economic Community.

Europe's most recent manifestation of this view is the EU Data Privacy Directive (Data Privacy Directive, 1995), from which springs the Safe Harbor Agreement. It represents a comprehensive, coherent perspective on personal data privacy, as opposed to the more ad hoc perspective in the US. The Directive governs the collection, storage, manipulation, use, and disclosure of personal data, defined as information about an identified or identifiable individual that is recorded in any form. It requires that transfers of personal information to non-EU countries take place only if they provide an "adequate" level of privacy protection for EU citizens. Transfers to countries not providing adequate protection are, in theory at least, prohibited.

III. PRINCIPLES STATED IN THE SAFE HARBOR AGREEMENT

After two years of sometimes rancorous negotiation, the Commerce Department agreed with the EU Commission on a set of principles laying out how the trading partners recognize the right to data privacy. The principles, embodied in the Safe Harbor Agreement, provide the framework that allows US organizations to satisfy the EU Directive's privacy requirements and simultaneously to ensure that personal data flows to the US are not interrupted. Thus, the Agreement acts as a mechanism enabling the Commerce Department to certify that participating US companies meet the requirements for adequate protection of EU citizens' privacy. US firms promising to adhere to the principles are posted on the Commerce Department's website (www.ita.doc.gov/ecom).

Seven principles form the basis of the Agreement:

1. Notice. An organization must inform individuals about the purposes for which it collects and uses information about them. It must also provide information about how individuals can contact the organization with any inquiries or complaints, the types of third parties to which it discloses the information, and the choices and means the organization offers for limiting the information's use and disclosure.

2. Choice. An organization must offer individuals the opportunity to choose, called *opt out*, if and how personal information they provide can be used or disclosed to third parties. It must provide individuals with clear and conspicuous, readily available, and affordable mechanisms to exercise this opt-out option. Individuals are to have an opt-in right, too, in which they agree before the fact to data transfers involving such sensitive information as medical/health data, racial or ethnic origins, political opinions, religious or philosophical beliefs, union membership, or information about their sex lives.

3. Onward Transfers. Organizations may disclose personal information only to third parties consistent with the principles of Notice and Choice. If an organization has not provided choice because the proposed data usage is compatible with the original purpose for which data were collected, it must ascertain that the third party subscribes to the safe harbor principles or that the third party promises at least the same level of privacy protection found in the principles.

4. Security. Organizations creating, maintaining, using, or disseminating personal information must take reasonable precautions to assure reliability for its intended use. They must also take reasonable precautions to protect the information from loss, misuse, and unauthorized access, disclosure, alteration, and destruction.

5. Data Integrity. Consistent with the principles, organizations may process personal information relevant only to the purposes for which it was gathered. To the extent necessary for those purposes, an organization should take reasonable steps to ensure that data are accurate, complete, and current.

6. Access. Individuals must have reasonable access to personal information about themselves that an organization holds and must be able to correct, amend, or delete information that is inaccurate. Reasonableness of access depends on the nature and sensitivity of the information collects, its intended uses, and the expense and difficulty of providing access to the information.

7. Enforcement. In order to ensure compliance, there must be readily available and affordable recourse mechanisms for handling individuals' complaints and disputes, and for awarding damages where applicable law so provides. Procedures must also be in place to verify that safe harbor organizations are in fact adhering to the principles; sanctions must be in place with sufficient rigor to ensure compliance.

IV. UNCERTAIN IMPACT

At this very early stage, many US organizations are uncertain about the impact of the EU-required "adequacy" standard on personal data transfers from

the EU to the US. US businesses in particular are concerned that an exchange of information, like point-of-sale data, marketing databases, and personnel records, might now cross over into the realm of privacy protection, thereby hindering cost-efficient data transfer to the US.

Such transfers are the lifeblood of many organizations and the underpinnings for all electronic commerce, including late-starting e-commerce in Europe. In particular, multinational corporations routinely share among their different offices a vast array of personal information, including simple items like personnel telephone directories and more sensitive items like personnel records, insurance/medical information, credit card billing information, and patient data for pharmaceutical research.

Of perhaps even greater, though longer-term, concern is the obvious intention of key congressional and administration admirers of the EU perspective to push for its wholesale adoption in this country. This, they believe, would provide a much-needed comprehensive privacy umbrella covering all sectors of American society, not just those dealing with data transfers to/from Europe.

The downside of such a national policy would be its forced change in how American organizations do business. For no matter how slow the policy's phase-in, certain heavy users of personal information, such as credit bureaus, direct marketers, fundraisers, catalogue printers, charities, and mailing list providers, would see their costs rise and profits fall. The ensuing shakeout might be far-reaching and painful.

V. WHAT SAFE HARBOR MEANS FOR HR MANAGERS

If the Safe Harbor Agreement withstands potential court challenges what should HR managers do? While there are as yet no easy answers, here are certain things that HR managers should do or at least be aware of.

1. Continue collecting and using data gathered anonymously from employees for routine statistical analysis and reporting, even data gathered from European operations. A key condition, though, is that the data processing cannot allow identification of individuals; it must aggregate only.

2. Begin notifying and giving the opt-out choice to individuals concerning their employers' wish to use their personal information collected through the employment relationship for non-employment purposes such as marketing communications. However, HR managers must not use opt-out decisions to restrict employment opportunities or take any punitive action against opting-out employees.

3. Do not offer notice and choice to individuals if an action at hand serves the organization's legitimate interests in making promotions, appointments, or other employment decisions.

4. Impose the principle of proportionality, or reasonableness, on requests for access to personal data owned by the organization. If information is used for decisions that significantly affect, say, an individual's employment, benefits, or financial position, the HR managers would have to disclose that information even if it is relatively expensive and burdensome to provide. HR managers would

probably wish to provide requested information that is not sensitive if it is readily available and inexpensive to provide. Yet if someone requests information that is not sensitive, but would be costly to provide, HR managers may wish to work with the individual to learn if there were alternative data that would satisfy just as well.

5. Start thinking about redesigning portions of the information systems, specifically the master employee databases, in order to accommodate the Agreement. This is especially true for US-domiciled multinational corporations which receive employee information routinely from Europe. In Europe, for instance, job applicants' resumes typically present information on marital status, gender, age, nationality, and so on. Since asking for such information is illegal in the US, implementing an international HR information system can be problematic for something as simple as resumes.

6. Continue making commitments in collective bargaining agreements regarding the use of employee information, even if an employee or union subsequently asserts that the firm breached the Safe Harbor Agreement and is thus engaged in an unfair labor practice. The Federal Trade Commission would most likely defer to the bargaining agreement and the traditional labor-law dispute-resolution procedure.

7. Finally, try to adhere to the spirit of the Agreement, if perhaps not the letter. After all, it is early yet and much interpretation needs to take place before even the experts know exactly what is going on.

VI. CONCLUDING REMARKS

Regulatory compliance is a great challenge for human resource practitioners in view of the hundreds of US federal, state, and local laws governing the field of human resource management. The challenge has become more difficult in the last decade as HR professionals move inevitably toward thinking and acting globally. Certainly, the Safe Harbor Agreement is a major thrust in that direction.

Indeed, it is likely that all HR managers must eventually abide by the Agreement, even if their organizations are not participants in it and do not or will not receive transfers of personal data from the EU. No HR operation will be untouched because the Agreement and its successors will probably form the basis for most future data privacy standards in this country.

VII. REFERENCES

Directive 95/46/EC of the European Parliament and the Council of the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995. Official Journal (L 281). ["1995 Data Privacy Directive."]

Released as "Safe Harbor Privacy Principles issued by US Department of Commerce on July 21, 2000.