



The Law Library of Congress

REPORT FOR CONGRESS

April 2011

Global Legal Research Center
LL File No. 2011-005536

EUROPEAN UNION

CORPORATE DISCLOSURE OF EMPLOYEE FINANCIAL DATA AND COMPATIBILITY WITH EUROPEAN UNION LAW

The Library of Congress
James Madison Memorial Building, 101 Independence Avenue, S.E., Room LM-240
Washington, DC 20540-3200
(202) 707-6462 (phone), (866) 550-0442 (fax), law@loc.gov (email)
<http://www.loc.gov/law>

LAW LIBRARY OF CONGRESS

EUROPEAN UNION

**CORPORATE DISCLOSURE OF EMPLOYEE FINANCIAL DATA AND
COMPATIBILITY WITH EUROPEAN UNION LAW**

Executive Summary

Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data is the basic framework legislation in the European Union (EU) on personal data protection. The Directive provides strong protections on processing of personal data of EU citizens. EU employee data fall within the definition of personal data. Processing of personal data through automatic or other means is prohibited unless it meets the safeguards provided by this Directive. Specifically, the disclosure of employee data falls within the ambit of processing and, hence, it is banned unless the criteria contained in the Directive are adhered to, including the unambiguous consent of the individual concerned. An individual who suffers damage due to unlawful processing is entitled to receive compensation, and controllers (those who process personal data) are responsible unless proven otherwise.

The Directive has extraterritorial application and prohibits the transfer of personal data to third countries that do not meet “an adequate level of protection.” The U.S. Department of Commerce and the European Commission have established the Safe Harbor Agreement to ensure that personal data transfers from the EU to the U.S. meet the required criterion. Multinational corporations that are or will be engaged in the processing of EU employee data have a legal obligation to adhere to the standards as contained in the Directive. In addition to the Safe Harbor agreement, which only applies to U.S. multinational corporations, companies may choose one of the following two methods to demonstrate that they meet the adequacy criterion: (a) by adopting contractual clauses; or (b) by adopting corporate binding rules.

I. Introduction

The European Union considers the right to the protection of one’s personal data as a basic human right distinct from the right to privacy. The Charter of Fundamental Rights, which is binding, provides in article 7 for the right to private and family life, whereas its article 8 ensures the right to the protection of one’s personal data as an autonomous right.¹

¹ Charter of Fundamental Rights of the European Union, as incorporated in the Treaty of Lisbon, entered into force Dec. 1, 2009, 2010 O.J. (C 83) 389, available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0389:0403:EN:PDF>.

Since 1995, at the European Union level, personal data of individuals are strictly regulated on the basis of Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (hereafter the Privacy Directive).² Under EU treaty rules, EU Members are required to transpose directives into national law within a prescribed period. In this case, the Privacy Directive entered into force in 1998, although some EU Members needed a longer period to implement the Privacy Directive into their domestic legal order. Its scope is broad and applies to the processing of personal data wholly or partially performed through automatic means or manually. Its territorial scope applies to the EU countries and to Iceland, Norway, and Liechtenstein. The directive has extraterritorial application because it requires that a transfer of EU personal data to third countries is possible only if the third country in question meets “an adequate level of protection.”³ Consequently, EU Members are required to ensure that data transfers to third countries that do not meet this criterion are prevented from taking place. Multinational U.S. corporations fall within the ambit of the extraterritorial application of the Directive and are obliged to adhere to the safeguards provided by the EU Privacy directive in processing EU employees’ personal data to the United States.

The European Commission has been reviewing the legal framework on protection of personal data and is contemplating new ways to strengthen data protection in view of challenges posed by new technologies that affect personal data.⁴

II. Overview of Legal Framework on Personal Data Protection

In addressing the question as to whether U.S. multinational corporations that may disclose employee data fall within the scope of the Privacy Directive, the preliminary question that must be addressed is whether employee data concerning such matters as salary, compensation, bonuses, etc., fall within the definition of “personal data,” as provided by the Privacy Directive.

A. Definition of “Personal Data”

The Privacy Directive broadly defines “personal data” as “any information relating to an identified or identifiable natural person” (the so-called data subject). An identifiable person is an individual who can be identified, either directly or indirectly, especially by reference to an

² Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter Privacy Directive), 1995 O.J. (L 281) 31, available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML>. Additional obligations for EU Members that are also members of the Council of Europe were imposed with the signing and ratification of the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108), Jan. 28, 1981, available at <http://conventions.coe.int/treaty/en/treaties/html/108.htm>.

³ Privacy Directive art. 26.

⁴ See *Communication from the Commission to the European Parliament, the Council, and the European Economic and Social Committee and the Committee of the Regions on A Comprehensive Approach on Data Protection in the European Union*, COM (2010) 609 final, available at http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf.

identification number or to one or more aspects specific to his physical, physiological, mental, economic, cultural, or social identity. Although the Directive does not specifically include employee data, such as salaries, compensation, bonuses, etc., the broad language employed—“any information”—leaves no doubt that employee data are, in fact, personal data.

The Working Party that was established on the basis of article 29 of the Privacy Directive and is tasked with examining questions arising from the application of the Directive has issued an opinion on this exact issue. Its Opinion No. 8/2001 on the Processing of Personal Data in the Employment Context confirms that employees are data subjects to which the Privacy Directive applies, that “many activities performed routinely in the employment context entail the processing of personal data of workers,” and that “any collection, use or storage of information about workers by electronic means will almost certainly fall within the scope of the data protection legislation.”⁵

Other definitions relevant to the issue at hand are those for “processing” and “controller.” Pursuant to the Directive, “processing” means “any operation or set of operations which is performed upon personal data, whether or not by automatic means.”⁶ It contains a nonexhaustive list of operations that includes “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.”⁷ A “controller” is “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.”⁸

B. Sensitive Data

In addition, corporations, by processing employee financial data, may reveal data related to one’s racial or ethnic origin or data pertaining to health, sexual orientation, or membership in trade unions. Processing of such data is prohibited by the Privacy Directive, subject to some exceptions, for example, when the individual concerned grants his explicit consent. However, the Directive allows EU Members to provide otherwise. Consequently, corporations must ascertain whether the national law on data protection completely bans the processing of sensitive data.⁹

C. Rights of the Data Subject

Among the rights afforded to the data subject is the right of access provided for in article 12 of the Privacy Directive. This right encompasses information to be provided to the data

⁵ Article 29 Working Party Opinion 8/2001 on the processing of personal data in the employment context, at 2 (Sept. 13, 2001), available at <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2001/wp48en.pdf>.

⁶ Privacy Directive art. 2(b).

⁷ *Id.*

⁸ *Id.* art. 2(d).

⁹ See also William A. Tanenbaum & Catherine Youssef Kassenoff, *Privacy and Data Protection: Collecting Employee Data in Europe*, N.Y.L.J., June 2007), http://www.kayescholar.com/news/publications/2007036/res/id=sa_File1/Tanenbaum_W_CollectingEmployeeDataInEurope.pdf.

subject regarding any processing of his data, purposes of processing, categories of data, and recipients of data.

Employees who themselves provide personal data to the controller for the purpose of processing are entitled to be provided with information as to the identity of the controller, the purpose of processing personal data, the recipients of data, existence of the right of access to his data, and the right to correct his data.¹⁰ If personal data have not be obtained from the data subject himself, then the controller or his representative is required to provide the data subject with the information provided above when recording personal data or prior to disclosing personal data to a third party.¹¹ In the second case, such data can be further processed for statistical purposes without the requirement of informing the data subject.¹²

D. Applicability of National Law

EU Members are required to apply the national law on the protection of personal data in the following cases:

- (a) When the processing takes place in the context of activities of an establishment of the controller within the jurisdiction of the EU Member concerned;
- (b) When the controller is not established within the territory of an EU Member but in a place where its national law applies as a matter of public international law; and
- (c) When the controller is not established in the EU territory, but for the purposes of processing data makes use of equipment that is situated in the territory of an EU Member.¹³

E. Basic Principles on the Processing of Employee Personal Data

In processing personal data of employees, multinational corporations must adhere to the following principles, arising from the Privacy Directive:

- **Finality:** Data must be collected for an explicit, specific, and legitimate purpose.
- **Transparency:** Employees must be informed of data collected and the purpose of collection.
- **Legitimacy:** Processing must be occur for a legitimate reason pursuant to article 7 of the Directive.
- **Proportionality:** Personal data collected must be adequate, relevant, and not excessive in relation to the purpose of collection.

¹⁰ Privacy Directive art. 10.

¹¹ *Id.* art. 11(1).

¹² *Id.* art. 11(2).

¹³ *Id.* art. 4.

- Accuracy and retention of the data: Employment records must be accurate and up to date. False or inaccurate data must be corrected.
- Security: Personal data must be secured through the adoption of technical measures to guarantee such security. Unauthorized access and disclosure must be prohibited.¹⁴

With regard to the issue of consent, the Working Party has opined that “it is misleading, if the employer seeks to legitimize this processing through consent.” Employers should rely on consent only when the employee “has a genuine free choice and is able to withdraw the consent without detriment.”¹⁵

The Working Party further noted that, pursuant to article 25 of the Directive, the transfer of employee data to a third country is possible only if the third country meets the “adequacy criterion.”¹⁶

F. Notification Requirements

Prior to the processing of personal data, a controller or his representative is required to notify the national supervisory authority established by each EU Member.¹⁷ National authorities are responsible for monitoring the application of the national law on data protection. The notification must include certain data, including the identification of the controller, the purpose of processing, the category of data to be processed, and the recipients of the data.¹⁸

G. Transfer of Personal Data to Third Countries Outside the EU

Transfers to a third country of personal data that are undergoing processing or will be processed after being transferred are prohibited, unless the third country in question meets an “adequate level of protection.”¹⁹ There are some derogations to this rule. Thus, national law may provide that a transfer of personal data to a third country that does not meet the adequacy criterion is possible on several grounds, including *inter alia* the following:

- Where the individual has granted his unambiguous consent to the proposed transfer;
- Where the transfer is necessary for the performance of a contract between the individual and the controller; and
- Where the transfer is necessary for the protection of the vital interests of the individual.²⁰

¹⁴ Working Party Opinion 8/ 2001, *supra* note 5, at 3.

¹⁵ *Id.*

¹⁶ *Id.* at 4.

¹⁷ Privacy Directive art. 18.

¹⁸ *Id.* art. 19.

¹⁹ *Id.* art. 25(1).

²⁰ *Id.* art. 26(1).

A transfer of EU employee data from a subsidiary company in France to its parent company in the United States would fall within the scope of the Privacy Directive because it involves transfer of EU employee data and the processing occurs within the context of activities of an establishment of the controller that is located in the territory of an EU Member State. Data protection authorities that have been designated by the EU Members to ensure the implementation of the Directive may impose heavy fines for violations of the national law on data protection. For example, in 2004, the Spanish Data Protection Authority imposed a fine of 840,000 Euros (at that time, approximately US\$900,000) on an organization for transferring customer data to a subsidiary organization.²¹

III. Means for Legally Transferring EU Personal Data by U.S. Corporations

To ensure an adequate level of protection of personal data to third countries outside the EU, corporations and other bodies have the following three options: (a) Safe Harbor principles, which apply only in the United States; (b) standard contractual clauses; and (c) binding corporate rules. These are characterized as tools that have an internal and external legal aspect and provide legal certainty and assurance that data are protected pursuant to safeguards provided by the Privacy Directive.²²

A. Safe Harbor Principles

The Safe Harbor Agreement is an agreement concluded by the European Commission and the U.S. Department of Commerce.²³ It is open to any 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. Upon committing to Safe Harbor principles, companies must adopt a privacy policy statement that must be renewed annually. By participating in the Safe Harbor, there is a presumption that companies meet the adequate security standard imposed by the EU Privacy Directive. The FTC supervises adherence to the Safe Harbor principles by companies.

B. Model Contractual Clauses

Corporations may use standard contractual clauses established by a decision of the European Commission in 2001²⁴ and updated in 2004.²⁵ Under both decisions, EU Members are

²¹ Morrison & Foerster, *EU Data Protection Requirements: An Overview for Employers* (Client Alert, Mar. 9, 2004), available at <http://www.mofo.com/pubs/xpqPublicationDetail.aspx?xpST=PubDetail&pub=7569>.

²² Working Document on Frequently Asked Questions (FAQs) Related to Binding Corporate Rules, (adopted June 2008; revised in 2009 by the Article 29 Data Protection Working Party, *infra* note 28).

²³ *Welcome to the U.S.-EU Safe Harbor*, EXPORT.GOV, http://www.export.gov/safeharbor/eu/eg_main_018365.asp (last updated Mar. 31, 2011). See also *Frequently Asked Questions (FAQs)*, EXPORT.GOV, <http://www.export.gov/faq/index.asp>.

²⁴ Commission Decision 2001/497/EC on Standard Contractual Clauses for the Transfer of Personal data to Third Countries Under Directive 95/46/EC, 2001 O.J. (L 181) 19, available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2001:181:0019:0031:EN:PDF>.

obliged to recognize that corporations that use the standard clauses in contracts regulating the transfer of personal data to third countries meet the “adequate level of protection” of data. The use of contractual clauses is voluntary.

C. Binding Corporate Rules

The Article 29 Working Party deems binding corporate rules (BCRs) as a useful tool for multinational companies and other groups to ensure compliance with the Privacy Directive. The specifics of such rules are contained in two Working Documents: (a) the 2003 Working Document 74: Transfers of Personal Data to Third Countries: Applying Article 26(2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers;²⁶ and (b) the 2005 Working Document 108: Establishing a model checklist application for approval of Binding Corporate Rules.²⁷ In addition, in 2008, the Working Party adopted Frequently Asked Questions (FAQs) Related to BCRs to facilitate the application of the above two documents.²⁸

To ensure that EU personal data are securely and legally transferred, U.S. companies usually adopt either contractual clauses or BCRs. The Safe Harbor framework is less popular, because it subjects employers to the enforcement authority of the FTC.²⁹

IV. Concluding Remarks

The protection of personal data of individuals is considered a basic human right and is guaranteed by the EU Charter of Fundamental Rights and the Council of Europe Convention on the Processing of Personal Data. Employee data are personal data and fall within the scope of the Privacy Directive, which stipulates certain safeguards for the processing of personal data. Processing is prohibited unless the criteria established by the Directive are met. In addition, the transfer of personal data to a third country outside the EU is prohibited unless the third country meets the “adequacy criterion.” In the United States, corporations have three means to ensure that they meet the strict standards of processing EU employee data: (a) the Safe Harbor framework, (b) contractual rules, or (c) binding corporate rules.

²⁵ Commission Decision 2004/915/EC Amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the Transfer of Personal Data to Third Countries, 2004 O.J. (L 385) 74, available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004D0915:EN:NOT>.

²⁶ Article 29 Data Protection Working Party, Working Document 74, Transfers of Personal Data to Third Countries: Applying Article 26(2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers (adopted June 3, 2003), available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2003/wp74_en.pdf.

²⁷ Article 29 Data Protection Working Party, Working Document 108, Establishing a Model Checklist Application for Approval of Binding Corporate Rules (adopted Apr. 14, 2005), available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp108_en.pdf.

²⁸ The FAQs were revised in April 2009. Article 29 Data Protection Working Party, Working Document on Frequently Asked Questions (FAQs) related to Binding Corporate Rules (Apr. 8, 2009), available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp155_rev.04_en.pdf.

²⁹ Sebastien Ducamp et al., *Recent Developments in EU Employee Privacy Law*, PRIVACY & DATA SECURITY L.J. 476 (Apr. 2007).

Prepared by Theresa Papademetriou
Senior Foreign Law Specialist
April 2011