The Legal Transfer of Employment-Related Data To Outside the European Union: Is It Even Still Possible?

JÖRG REHDER AND ERIKA C. COLLINS*

I. Introduction

Current European Union (EU) data privacy laws place multinational companies in an unenviable position. On one hand, the laws are broadly worded yet strict, and on the other, a multitude of questions regarding application and enforcement remain unanswered. As a result, companies that make an effort to comply with data privacy laws—which, as this article will discuss, is by no means a given—face a complex situation. To make matters worse, the field of data privacy is a moving target. To put it colloquially, many companies are talking about data privacy,[1] but not every company is "doing" data privacy,[2] and if a company is doing data privacy, it is very possible that, through no fault of its own, the company is not doing it correctly.[3] With this in mind, the authors thought that an article

*Mr. Rehder is an Attorney at Law and Solicitor (England and Wales) with Jones Day (Frankfurt, Germany). He is specialized in cross-border M&A, corporate, commercial and labor and employment matters. Ms. Collins is Of Counsel with Paul, Hastings, Janofsky & Walker LLP (New York) and Chair of the firm's International Employment Law Group.

1. According to a recent survey, 42% of company managers are aware of data protection laws and data protection authorities. Special Eurobarometer 196, *Data Protection* (European Opinion Research Group), Dec. 2003, at 48, *available at* http://www.europa.eu.int/comm/public_opinion/archives/ebs/ebs_196_data_protection.pdf [hereinafter Special Eurobarometer 196].

2. According to the results of an EU company survey conducted from September 15, 2003, to October 3, 2003, 39% of respondents within the EU said that controllers do not fully observe data protection laws because of "lack of knowledge of legislation" while 54% of respondents attributed the non-adherence to factors such as the risk of "being caught is low" (28%), implementing the necessary measures at the company would be too time consuming (17%), and lack of flexibility of the law (9%). The remaining 7% responded either with "Other" or "Don't Know/No Answer." Flash Eurobarometer 147, *Data Protection in the European Union* (European Opinion Research Group) Dec. 2003, *available at* http://www.europa.eu.int/comm/public_opinion/flash/fl147_data_protect.pdf, at 51-52.

3. "The lack of clarity for both employers and employees of the many national policies and laws on workplace privacy is creating an unacceptable risk for business, particularly multinational business." *Employee privacy, data protection and human resources*, ICC Policy Statement, Doc. No. 373-22/112 (Dec. 4, 2003), *available at* http://26konferncja.giodo.gov.pl/data/resources/KunerC_paper.pdf. One aspect of data protection that has created

discussing data privacy practices that have evolved over the years in the employment arena, as well as analyzing what the future may hold, would be timely.

The EU passed the Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (Directive)[4] nearly ten years ago.[5] Despite the clearly stated purpose of the Directive—to ensure that "member states [ ] protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data"[6]—companies and advisors often find themselves in uncharted territory when processing or transferring data, preparing privacy policies, or advising on data privacy matters. Further, though the Directive was not meant to apply specifically to data within the employment context,[7] it quickly became clear that the "processing"[8] of this type of information—much of it personal to employees—is also subject to the Directive, meaning employers need to follow certain guidelines when processing employee data. In essence, employers must treat such data as employees' personal property. Failure to do so exposes a company to potential liability.

The Directive concerns not only the "processing" of personal data, but also the "transferring" of personal data from EU countries[9] to non-EU countries. If a non-EU country does not provide for "adequate protection,"[10] as determined by the EU, then a company

---

havoc for companies and advisors is the issue of which member state's laws apply to a particular data processing. One example is "Article 4 of the Directive dealing with applicable law, which has become the subject of increasing criticism, as companies have come to find that it can be nearly impossible to determine with certainty which member state law or laws apply to a specific act of data processing in many common business situations." *See* Christopher Kuner, *The Commission's First Report on Implementation of the E.U. Data Protection Directive*, WORLD DATA PROTECTION REPORT (Aug. 2003), at 4.

4. Council Directive 95/46/EC 1995 O.J. (L 281) 31, 31-50 [hereinafter Directive].

5. The Directive was issued on October 24, 1995. *Id.* at 31. Of the fifteen member states of the EU prior to May 1, 2004, France was the last country to harmonize the Directive into its national law. Law No. 2004-801 of Aug. 6, 2004, J.O., Aug. 7, 2004; JCP—(Fr.) (amending Law No. 78-17 relating to Computers, Files, and Liberties to harmonize to the Directive). *See infra* note 17 as to the status of the harmonization process in the new EU member states.

6. Directive, *supra* note 4, art. 2(a). at 38.

7. The Directive refers to the processing of "personal data," whereby personal data is broadly defined as "*any* information relating to an identified or identifiable natural person." *Id*, art. 2(a), at 38.

8. The Directive defines "processing" in intentionally broad terms as "any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction." *Id.* art. 2(b), at 38.

9. For purposes of this article, the European Economic Area (EEA) countries, Iceland, Norway and Liechtenstein, are deemed to be part of the EU since the Directive also applies in these countries. Pursuant to article thirty-six of the Agreement on the EEA, version of May 5, 2004, and section 5e of Annex XI thereof, the EEA countries notified the Commission that the Directive shall apply in their respective states. Decision of the EEA Joint Committee No. 83/1999 of June 25, 1999, amending Protocol 37 and Annex XI to the EEA Agreement, 2000 O.J. (L 296) 41, *available at* http://europa.eu.int/eur-lex/pri/en/oj/dat/2000/l_296/l_29620001123en00410043.pdf.; *see also* EEA Supplement No. 43 (Nov. 23, 2000), at 112(I), 81 Del 2 (N) (entered into force on July 1, 2000), *available at* http://secretariat.efta.int/Web/Publications/EEASupplement/NO/EEASupplement2000/Su43n.pdf. Iceland, Norway, and Liechtenstein enacted respective data privacy laws available for review at http://europa.eu.int/comm/internal_market/privacy/links_en.htm.

10. "Adequate protection" is not specifically defined in the Directive; however, it states that the adequacy of the level of protection . . . shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country

generally may not transfer data to that country unless the company has taken other approved measures.

Before delving into the subjects of "processing" and "transferring" data, it is helpful to compare quickly the EU and U.S. approaches to data privacy. The EU subscribes to a general, all-encompassing "one size fits all" approach.[11] Its focus is to protect the fundamental human right of privacy. The EU also regulates the export of data outside its borders[12] to ensure that a person's right to privacy is not invaded. The United States has not taken such a broad-based approach, but instead has taken a sectoral, patchwork approach that consists primarily of reacting to specific data privacy issues that have arisen in various industries. Both U.S. state and federal governments have addressed these issues by enacting various statutes[13] and regulations. Put simply, the U.S. data privacy laws are generally not as onerous as those of the EU. The attacks of September 11, 2001, "have further weakened Washington's will to protect data. [In fact, t]hrough new laws and new offices, Washington now has more unfettered access to citizens' data than ever before."[14] The relative ease of processing data in the United States by the public sector is also prevalent in the private sector, at least when compared to the EU.

The EU and U.S. approaches to data privacy clearly are not reconcilable with one another.[15] To further complicate matters, as will become apparent throughout this article, the

---

of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country. Directive, *supra* note 4, art. 25(2), at 45.

11. For a discussion comparing the EU and U.S. approaches to data privacy, *see* Graham Pearce & Nicholas Platten, *Orchestrating Transatlantic Approaches to Personal Data Protection: A European Perspective*, 22 FORDHAM INT'L L.J. 2024 (1999).

12. *Id.* at 2027.

13. *See, e.g.*, Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501-6506 (2000); Fair Credit Reporting Act, 15 U.S.C. § 1681 *et. seq* (2004); Video Privacy Protection Act of 1988, U.S.C. § 2701 *et. seq.* (2004); Identity Theft and Deterrence Act of 1998, Pub. L. No. 105-318, 112 Stat. 3007 (1998) (largely codified at 18 U.S.C. § 1028 (2004) and 28 U.S.C. § 994); Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, 110 Stat. 1936 (1996).

14. David Scheer, *Europe's New High-Tech Role: Playing Privacy Cop to the World*, Wall. St. J. (October 10, 2003) at A1. One such new law is the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56, 115 Sta. 272 (2001). For a more complete discussion regarding the USA PATRIOT Act, *see* Justin F. Kollar, *USA Patriot Act, the Fourth Amendment, and Paranoia: Can They Read this While I'm Typing It?* 3 J. HIGH TECH L. 67 (2004); Jeremy Smith, Comment, *The USA Patriot Act: Violating Reasonable Expectations of Privacy Protected by the Fourth Amendment without Advancing National Security*, 82 N.C.L. Rev. 412 (2003); Eric J. Gouvin, *Bringing Out the Big Guns: The USA Patriot Act, Money Laundering, and the War on Terrorism*, 55 BAYLOR L. REV. 955 (2003); Tracey T. Gonzalez, *Individual Rights versus Collective Security: Assessing the Constitutionality of the USA Patriot Act*, 11 U. MIAMI INT'L & COMP. L. REV. 75 (2003); Peter G. Madrinan, Note, *Devil in the Details: Constitutional Problems Inherent in the Internet Surveillance Provisions of the USA Patriot Act of 2001*, 64 U. PITT. L. REV. 783 (2003).

15. The United States, however, did pass a data privacy law in 1974 to protect individuals from invasion of privacy by the federal government by placing limitations on the disclosure of certain information concerning individuals. Privacy Act of 1974, 5 U.S.C. § 552a (Supp IV 1974). The Privacy Act of 1974 differs significantly from the Directive in that the former applies only to the use and dissemination of records by the U.S. federal government while the Directive applies to the processing of transfer by any party, whether public or private. For a more complete discussion on the Privacy Act of 1974, *see* Jerome J. Hanus & Harold C. Relyea, *A Policy Assessment of the Privacy Act of 1974*, 25 AM. U.L. REV. 555 (1976); Julianne M. Sullivan, Comment, *Will the Privacy Act of 1974 Still Hold Up in 2004? How Advancing Technology Has Created a Need for Change in the "System of Records" Analysis*, 39 CAL. W.L. REV. 395 (2003).

treatment of data privacy is not uniform among the individual EU member states. The EU has, however, established certain procedures to transfer data outside the EU. These procedures are the subject of this article.

II. General Provisions of the Data Privacy Directive

Until May 1, 2004, the following member states comprised the EU: Austria, Belgium, Denmark, Finland, France, Germany, Greece, Ireland, Italy, Luxembourg, the Netherlands, Portugal, Spain, Sweden, and the United Kingdom. The EU expanded to 25 countries on May 1, 2004, with the addition of ten states from Eastern and Southern Europe, specifically Cyprus, the Czech Republic, Estonia, Hungary, Latvia, Lithuania, Malta, Poland, Slovakia, and Slovenia.[16]

The EU passed the Directive in 1995 in an effort to harmonize various data protection regimes among the member states, many of which had well-established data protection statutes years before the Directive came into effect.[17] To realize this harmonization goal, the Directive outlines general data protection principles that individual member states must observe. Though the individual laws of each member state dictate the data privacy policies of that particular member state,[18] the Directive is an important tool, as it is the key document upon which all member states must base their respective data privacy laws.

16. The geographic scope of the Directive expanded accordingly. According to a report by the European Commission,

> [i]n line with the Copenhagen criteria, all candidate countries are committed to transposing Directive 95/46/EC by the time of accession. To date, all have passed legislation in this field ... In the 10 countries that have signed the Treaties of Accession, the legislation in place incorporates most of the key elements of the Directive. However, further efforts are needed to bring this legislation fully into line with all provisions of the Directive.

Report from the Commission: First Report on the Implementation of the Data Protection Directive (95/46/EC), May 15, 2003, at 13, *available at* http://europa.eu.int/eur-lex/en/com/rpt/2003/com2003_0265en01.pdf. *See* http://europa.eu.int/comm/internal_market/privacy/links_en.htm (providing information on current data privacy statutes of the new EU member states). The Copenhagen criteria is referred to as such because these criteria were established at the 1993 Summit of the European Council in Copenhagen, Denmark. Candidate countries were supposed to satisfy these various political and economic criteria before they could become EU member states. At the time of this writing, while all new EU member states have taken action to harmonize the Directive into their respective national laws, most of the new EU states are not yet fully compliant with the Directive and are in the midst of negotiations and discussions with the Commission to correct their respective shortcomings. *See id.*

17. For example, Germany enacted a federal data protection statute effective in its entirety already on January 1, 1979. Bundesdatenschutzgesetz ("BDSG"), v. 27.1.1977 (BGBl. I S.201) (F.R.G.) [hereinafter German Federal Data Protection Act]. Prior to that, two German states (*Länder*) enacted data protection statutes at the state level: Hesse in 1970 and Rheinland-Palatine in 1974. Hesse's general data protection statute was the first such statute passed in the world. PETER GOLA & RUDOLF SCHOMERUS, BUNDESDATENSCHUTZ KOMMENTAR 55 (C.H. Beck, Munich, 8th ed. 2005) [hereinafter GOLA & SCHOMERUS]. France also enacted the statute relating to Computers, Files and Liberties in 1978. *See* Law No. 78-17 of January 6, 1978, J.O. January 7, p. 227, as amended. Many of the general principles set out in that statute were similar to those set forth in the Directive. For example, employers were required to inform employees of their rights at the time they collected the data. It is probably for this reason that harmonizing the Directive into its national laws was not one of France's political priorities.

18. The EU Council's and Commission's actions may be in the form of directives, regulations, decisions, recommendations, or opinions. Treaty of Amsterdam Amending the Treaty on European Union, the Treaties Establishing the European Communities and Related Acts, art. 249, 1997 O.J. (C 340) 1, *available at* http://

A basic tenet of the Directive is that employers must ensure that all personal data concerning employees is processed in accordance with the following "data protection principles":[19]

1) Accuracy and Retention of Data: Data must be accurate and kept current and any erroneous data must either be erased or corrected.
2) Awareness of the Staff: Any employee who is involved in processing personal data must be made aware of the data protection requirements, receive proper training, and be aware of the obligations regarding protecting employees' privacy.
3) Finality: Personal data may be processed only for specific, stated purposes and may not be processed for any other incompatible purpose.
4) Legitimacy: Personal data may only be processed for "legitimate" purposes as set forth in article 7 of the Directive (see below).
5) Proportionality: Processing of personal data may not be excessive in relation to the purpose(s) for which it was collected.
6) Security: The employer must have appropriate security measures in place to ensure that personal data is kept safe from unauthorized access or distribution, e.g., the employer must have appropriate technical and organizational measures in place.
7) Transparency: Employers must notify employees about what data the employer is collecting about them (both directly and from other sources), must give employees access to such data, and let them know for what purpose they are processing the data.[20]

---

www.w3.org/WAI/EO/EuropAmst.pdf. Since the data privacy directive is in the form of a "directive," it is not directly applicable, meaning each EU country must "harmonize" (or enact) the Directive into its national law; or as set forth in article 249 of the Treaty of Amsterdam, "[a] directive shall be binding as to the result to be achieved, upon each member state to which it is addressed, but shall leave to the national authorities the choice of form and methods." *Id.* This is in contrast to a "regulation," which is directly applicable in all EU member states without necessitating any further legislative action. One example where a country failed to harmonize the Directive correctly into its national law relates to article 25(4) of the Directive as harmonized into German national law, in particular section 4c(2) of Germany's Federal Data Protection Act. The Directive states where the Commission finds that a third country does not ensure an adequate level of protection, member states shall take measures necessary to prevent any transfer of information to such a third country. Directive, *supra* note 4, art. 25(4), at 46. However, section 4c(2) of Germany's Federal Data Protection Act states that "transfers of personal data to *bodies*" may be authorized if the employer adduces adequate safeguards with respect to the privacy and exercise of the corresponding rights. German Federal Data Protection Act, *supra* note 17, at § 4(c)(2). In essence, the Directive requires that the *third country in which the receiving body is located* must provide adequate protection, while the German legislation requires only that the *receiving body* provide adequate protection—a significant difference. *See* Christoph Rittweger & Bjorn Weisse, *Unternehmensrichtlinien fur den Datentransfer in Drittlander*, COMPUTER UND RECHT, Feb. 15, 2003, at 142, 147.

19. *See* Article 29-Data Protection Working Party Opinion 8/2001 On the Processing of Personal Data in the Employment Context, Sept. 13, 2001 (5062/01/EN/Final WP 48), at 3, *available at* http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2001/wp48en.pdf [hereinafter Working Party Opinion 8/2001]; (setting forth data protection principles derived from Article 6 of the Directive) *see also* Directive, *supra* note 4, art. 6, at 40. The article 29 Working Party is an independent, advisory board comprised of the data protection authorities of each of the member states. It does not have rule-making authority. The article 29 Working Party was established in article 29 of the Directive. For more information regarding the article 29 Working Party, *see* CHRISTOPHER KUNER, EUROPEAN DATA PRIVACY LAW AND ONLINE BUSINESS 9-10 (Oxford University Press 2003).

20. While not an employment-law related case, a U.K. Court of Appeals recently held that under the U.K.'s Data Protection Act 1998 an individual may not access data merely because reference is made to that individual as part of the data. Instead, the test is whether there is some element of "relevance or proximity" to that

Of the seven principles listed above, "legitimacy" is most open for interpretation and thus has been most troublesome for employers to apply.

According to the Directive, one manner of legitimizing data processing is to obtain the employee's unambiguous consent.[21] However, whether an employee has given such consent may not be easy to determine. For example, does the conclusion of a written employment agreement that includes consent to process data in the text constitute unambiguous consent? The answer depends on the jurisdiction and the type of data the employer will process, but probably not. In many EU jurisdictions, mere inclusion of a consent clause in an agreement does not suffice unless consent is prominent.[22] Also, an employer may not tie an employee's "unambiguous" consent to process data to that employee being hired or remaining employed, as such consent has not been given freely.[23] An employee also has the right, with some limitations,[24] to withdraw consent at any time. Finally, according to the article 29 Working Party, employers should use consent for the processing of data only as a "fall back

---

individual, more specifically, whether the data is biographical in nature and focuses on that particular individual. Only then will that person have a right of access. *Durant v. Financial Servs. Auth.*, [2004] F.S.R. 28, [2003] EWCA 1746 (U.K.). Employers in the United Kingdom have received this opinion favorably as employees have sometimes inundated employers with unreasonable requests for data. *Durant* gives U.K. employers some additional leeway in denying such requests for information.

21. Directive, *supra* note 4, art. 7(a), at 40.

22. In Spain, the consent of any person whose personal data is to be processed must generally be "unambiguous." Organic Law 15/1999 of 13 December on the Protection of Personal Data (B.O.E. 1999, —), *available at* https://www.agpd.es/upload/Ley%20Org%E1nica%2015-99_ingles.pdf [hereinafter Organic Law 15/1999]. If an employer collects personal data without the explicit consent of the employee, the employer may be guilty of a "serious infringement" of Spain's Data Protection Law. *See* discussion infra section III.B). *See also*, German Federal Data Protection Act, *supra* note 17, § 4(a)(1), which states that "[i]f consent is to be given together with other written declarations, it shall be made distinguishable in its appearance." The French data protection authorities are unofficially of the opinion that an employee's consent by its very nature cannot be given freely; however, there is no French case law or statute that confirms this opinion. In the United Kingdom, if an employer processes sensitive data, employers ". . . must bear in mind that . . . the consent must be explicit. This means the worker must have been told clearly what personal data are involved and the use that will be made of them. The worker must have given a positive indication of agreement, e.g., a signature. . . ." Employment Practices Data Protection Code: Part 4: Information About Workers' Health, at 20, *available at* http://ico-cms.amaze.co.uk/DocumentUploads/part%204%20employment%20code%20final.pdf [hereinafter U.K. Employment Practices Data Protection Code]. Under Finnish law,

> [t]he employer is only allowed to process personal data directly necessary for the employee's employment relationship which is connected with managing the rights and obligations of the parties to the relationship or with the benefits provided by the employer for the employee or which arises from the special nature of the work concerned. No exceptions can be made to the necessity requirement, *even with the employee's consent.*

Finland's Act on the Protection of Privacy in Working Life (759/2004), § 3, *available at* http://finlex.fi/pdf/saadkaan/E0010477.pdf.

23. For example, according to the U.K.'s Employment Practice Data Protection Code, ". . . the worker must have a real choice whether or not to consent and there must be no penalty imposed for refusing to give consent." U.K. Employment Practice Data Protection Code, *supra* note 22, at 20. This analysis is in line with the analyses of the other EU member states.

24. An employee's attempted withdrawal of consent may be invalid if there is no reasonable basis for the withdrawal and if the data are processed in performance of an agreement that has already been executed and to which the employee already gave its consent. GOLA & SCHOMERUS, *supra* note 17, at 171-72. These types of limitations on withdrawal, however, are quite rare and employers should rely on them only in extreme cases.

position."[25] In practice the consent form should be, at a minimum, a document separate from the employment agreement so that the employee signs each document separately, thereby indicating unambiguous consent.

Other than through consent, article 7 permits processing of data only if it is "necessary," as that term is used in the Directive. First, processing may be necessary in order for the employer to perform its contractual obligations vis-à-vis an employee (e.g., processing an employee's salary data). Processing data may also be necessary for an employer to comply with its legal obligation (e.g., processing an employer's data for the purpose of calculating the withholding tax). Finally, an employer may also need to process employee data to protect that employee's vital interests (e.g., an employer may compile medical data regarding the employee to protect the employee against particular hazards at the workplace). Article 7 of the Directive specifically permits each of the above.[26]

An employer may also process data if the necessity of such processing outweighs the employee's privacy interests.[27] There may be a fine line between what is "necessary" and what constitutes an invasion of an employee's privacy. As the following examples illustrate, an employer should err on the side of caution when considering whether to rely on this provision.

The first example comes from the area of due diligence. One concern that many employers have when selling a company is whether they may—or even want to—disclose information to the potential buyer without violating the data privacy principles. For example, the ages, years of service, and duties of the employees are basic information that any potential buyer will request during the due diligence phase of an acquisition. In Germany, sellers may only disclose information for due diligence purposes to the extent it is necessary for the realization of the transaction.[28] Thus, the practical effect is that the selling employer may only disclose information in stages. For example, during initial discussions the seller may disclose the number of employees at each site, their job duties, the aggregate salaries for each department, and the average years of service, which means the data is still "anonymous" (the seller has not yet disclosed data regarding the individual employees) during the initial stage. As negotiations proceed, the seller may provide the buyer with increasingly more information so the buyer can make an informed decision as to whether to proceed with the transaction.[29]

By contrast, Belgian and Spanish data protection authorities have in the past unofficially taken the stance that since employees do not contemplate that their employer will transfer data in connection with the sale of a company, the employer is permitted to transfer this data only with each employee's consent. In essence, when Belgian and Spanish data collection authorities collected the data, their purpose was not to make it available to potential buyers of the company.

As one could guess, it is becoming more common for sellers in the EU to use the data privacy laws as a ruse for not disclosing pertinent information to potential buyers, by relying on the argument that data privacy laws prohibit them from disclosing information. In fact,

25. Working Party Opinion 8/2001, *supra* note 19, at 23.
26. Directive, *supra note 4, art.* 7(b)-(d).
27. *Id.* art. 7(f).
28. German Federal Data Protection Act, *supra* note 17, § 28.
29. However, confidentiality agreements may also restrict the seller from disclosing certain information.

the motivating factor is that these sellers are not willing to disclose detailed information to potential buyers, often competitors, until they are certain that the transaction will indeed close.

Another example in which an employer may disclose information about its employees is for marketing purposes. It is incontrovertible that an employer has the right to disclose information regarding its employees for marketing purposes. For example, many companies share the names of their senior executives with customers, employees in the marketing department, or particular members of the research and development department. But the question of how much information an employer may disclose without obtaining the employee's consent remains unanswered. Again, as part of the balancing test, the employer must weigh what information it "needs" to disclose to satisfy its purpose of attracting customers. Disclosing the education levels of certain employees may be appropriate, as well as to the extent it is relevant, the various professional responsibilities held by an employee in the past. Employers, however, typically do not "need" to disclose an employee's personal information, such as past employers, years of service, or age. Of course, to reduce any risk of violating an employee's right to privacy, the employer should consider obtaining an employee's written consent before processing the information. This consent, as discussed above, may either be in the form of individual consent or, if the company has a works council, consent from the works council through a works agreement.[30]

The above examples concern the disclosure of information to unaffiliated third parties, such as potential acquirers of a target company or customers. The disclosure of information among affiliates, however, may also raise data privacy issues. To illustrate, many human resource departments have centralized their data for purposes of efficiency and thus use software for their global human resource needs. The obvious risk here is that other employees may access this information, such as salary, benefits, years of service, or medical history, without authorization. Employers should carefully ensure that unless a particular employee truly needs access to data regarding other employees, they are not given access to such data, even if both employees are in the same company or an affiliated company.

Employers must also be aware that processing certain types of "sensitive data" involves extremely stringent requirements. Article 8(1) of the Directive defines sensitive data as revealing: (1) racial or ethnic origin; (2) political opinions; (3) religious or philosophical beliefs; (4) trade-union membership; or (5) health or sex life. The basic proposition is that, with certain exceptions, processing of sensitive data by employers is prohibited[31] unless the employee consents in the form of "opting-in," meaning the employee gives his employer express consent to process such data. This differs from "opting out," which occurs when an employee is deemed to have given consent to certain processing unless he expressly prohibits the employer from processing the data.

30. Works councils are employee representative bodies. They are not to be confused with unions since these two bodies have different responsibilities and rights. A works council is comprised of the employees themselves. The duties of a works council are to ensure that an employer observes his responsibilities vis-à-vis the employees and to negotiate with management on personnel matters, such as the introduction of new working hours, manner of payment of wages, vacation policies, safety at the workplace issues, and the like. Agreements between the works council and management are in the form of works agreements. Neither management nor a works council may unilaterally modify a works agreement, instead, the two must mutually agree to amend a works agreement.

31. Working Party Opinion 8/2001, *supra* note 19, at 17.

Experience shows that many employers process at least some sensitive data almost unwittingly simply because this has become part of their "standard procedure." For most employers, processing such data has rarely caused problems in the past. Employers should review their need to continue to process such data, however, because many people, including employees, are concerned about third parties, such as employers, collecting information, resulting in a potential invasion of privacy.[32] Therefore, employers should not ignore the risk of an employee taking action against an employer based on an employer's unauthorized processing of sensitive data.

One additional issue that often arises is to what extent, if at all, must an employer notify data protection authorities before processing data. Under the Directive, member states must ensure that an employer notifies the data protection authorities "before carrying out any wholly or partly automatic processing operations."[33] To prevent making the Directive even more impractical than it already is, however, the Directive also provides for a number of exceptions to this requirement. To the extent permitted by national law, the exception most employers use to avoid having to notify data protection authorities of automated processing of data is to appoint a data protection officer within the company.[34] The officer's primary responsibilities are: (1) to ensure that the company complies with national laws; and (2) to keep proper records of data processing.[35]

III. Transferring Personal Data to Third Countries

The extraterritorial aspect of the Directive appears in articles 25 and 26, which provide that member states must ensure that personal data is not transferred to third, meaning non-EU, countries unless that country "ensures an adequate level of protection,"[36] or if another permissible transfer under article 26 is available. Only a few jurisdictions enjoy the "adequate protection" label provided by the EU, namely Switzerland,[37] Hungary,[38] Canada,[39] Argentina,[40] Guernsey,[41] and the Isle of Man.[42]

32. According to a survey conducted between September 1, 2003, and September 30, 2003, 32% of the respondents within the EU said that they "do not trust" employers to use employee-related data in an acceptable manner Special Eurobarometer 196, *supra* note 1, at 19. Although this is slightly better than in 1996,when 34% of the respondents said that they "do not trust" employers to use human resources data in an acceptable manner, the percentage of employees who will distrust their employers may very well increase over time as employees become increasingly aware of the type of data employers are collecting and transferring.

33. Directive, *supra* note 4, art. 18(1).

34. *Id.* § 18(2).

35. *Id.*

36. *Id.* art. 25(1).

37. Commission Decision 2000/518/EC 2000 O.J. (L 215) 1.

38. Commission Decision 2000/519/EC 2000 O.J. (215) 4. This Commission Decision is now moot since Hungary became a member state to the EU on May 1, 2004.

39. Commission Decision 2002/2/EC 2002 O.J. (L 2) 13, so long as the recipient of the data is subject to Canada's Personal Information and Protection and Electronic Documents Act.

40. Commission Decision C (2003) 1731.

41. Commission Decision 2003/821/EC, 2003 O.J. (L 308) 27.

42. Commission Decision 2004/411/EC, 2004 O.J. (L 151) 48.

A number of significant countries are missing from this list, notably Japan, Russia, Australia,[43] China, Brazil, India,[44] and important for purposes of this article, the United States. In fact, the EU views the United States as *not* ensuring an adequate level of data protection.[45] Thus, while it may be legal for EU entities to collect personal information and disclose it to affiliates within the EU, it may be *illegal* to transfer the same information to U.S. affiliates. The economic impact of disallowing companies to transfer personal data from the EU to the United States would be catastrophic because not only would doing so prohibit independent, third parties, including manufacturers and customers from these jurisdictions from sending data to one another, but affiliated companies in these jurisdictions would also be prohibited from doing so.

A. Compliance Mechanisms and Choices

Fortunately, procedures are available to EU employers so that they may legally transfer[46] data to persons located in jurisdictions that the EU has not concluded provide the requisite adequate protection; specifically, four methods are available, each of which carries distinct advantages and potential pitfalls. Of course, a company may also choose to ignore the Directive's principles, but this choice carries with it several risks, including exposure to potential civil judgments or even criminal prosecution.[47]

---

43. Article 29-Data Protection Working Party Opinion 3/2001 On the Level of Protection of the Australian Privacy Amendment (Private Sector) Act 2000, Jan. 21, 2001 (5095/00/EN/ WP40 final), *available at* http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2001/wp40en.pdf. The Article 29 Working Party concluded that Australia's legislation did not provide for adequate protection, in part because the Australian privacy legislation exempted certain employee records from the data privacy rules. Negotiations between the EU and the Australian government are proceeding at the time of this writing and it is hoped that Australia will meet the EU's requirements so that Australia will be deemed to provide adequate protection within the foreseeable future.

44. Eduardo Ustaran, *Offshore Outsourcing*, E-commerce Law and Policy, July 2003, at 14. At this time, only informal discussion are being held with representatives of India's government with respect to what steps India must take in order for the EU to recognize it as a country that provides adequate protection.

45. Working Party's Opinion 1/99 concerning the level of data protection in the United States concludes that the "current patchwork of narrowly-focused sectoral laws and voluntary self-regulation cannot at present be relied upon to provide adequate protection in all cases for personal data transferred from the European Union." Working Party Opinion 1/99 on the Protection of Individuals with Regard to the Processing of Personal Data, Jan. 26, 1999 (5092/98/EN/final/WP 15), at 2, *available at* http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp15en.htm. Many commentators believe that the United States does not have a comprehensive federal data privacy law comparable to the Directive since Americans are generally more wary of the government regulating data privacy and prefer self-regulation. *See* Stephen J. Kobrin, *Safe Harbours are Hard to Find: The Trans-Atlantic Data Privacy Dispute, Territorial Jurisdiction and Global Governance*, 30 Rev. of Int'l Stud. 111, 111-31 (2004).

46. The European Court of Justice recently held that the loading of data onto a website that is stored with a hosting provider in that same or another EU member state did not constitute a "transfer" of data within the scope of the Directive, even though people from other countries could access this data. *Bodil Lindqvist v. Åklagarkammaren i Jönköping*, 1 C.M.L.R. 20 (E.C.J. 2003). In the *Lindqvist* case, Ms. Lindqvist set up a website on her personal computer and provided information about her eighteen fellow parishioners of the Swedish Church in Alseda, Sweden. Some of the data included names and phone numbers of the parishioners as well as their occupations and hobbies. She had not obtained the consent of the parishioners before posting this information. The European Court held that this constituted a violation of the Directive's principles. However, even though people from other countries had access to the information, the posting of the information on the internet did not constitute the transferring of data to other countries so long as the hosting provider was located within the EU. *Id.*

47. Directive, *supra* note 4, arts. 22-24.

The four following compliance choices are available to employers when transferring data to countries without adequate protection:

(1) Standard contractual clauses;
(2) Self-certification under Safe Harbor;
(3) Codes of Conduct; and/or
(4) Exemptions under article 26 of the Directive.

These alternatives are discussed below with emphasis on the practicalities of each and their respective advantages and disadvantages.

1. *Standard Contractual Clauses*

To begin, companies may find it useful to use EU-approved standard contractual clauses to ensure that data transfers meet an adequate level of protection.[48] Of the alternatives available to companies transferring data outside of the EU, the use of standard contractual clauses is the most straightforward. Standard contractual clauses, as prepared by the EU, contain specific terms and conditions for the transfer of data from the EU transferor to the non-EU data recipient. The parties essentially are required to copy the terms of the standard contractual clauses verbatim and then fill in the blanks. Included as an integral part of the standard contractual clauses are the data quality principles that the contractual parties agree to observe.[49] While parties are free to draft additional terms to the contract, the EU does not permit parties to use limitations or clauses that contradict the purpose of the standard contractual clauses.[50]

There are two types of EU standard contractual clauses. The first is for the transfer of personal data from an employer (referred to as a controller) established in the EU (data exporter) to a party (also a controller) established in a third country (data importer).[51] The second is for the transfer of personal data from a controller (employer) to a processor of data, for outsourcing projects as an example, established in a third country.[52] The former is commonly referred to as "Controller to Controller" while the latter is referred to as "Controller to Processor."

Authorizing each set of standard contractual clauses, article 26(2) of the Directive states that

> a Member State may authorize a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of article 25(2), where the controller adduces adequate safeguards with respect to the protection of privacy and

48. These standard contractual clauses are authorized under article 26(4) of the Directive and were approved by the European Commission in two decisions. *See* Commission Decision 2001/497/EC, 2001 O.J. (L 181) 19 [hereinafter Commission Decision 2001/497/EC] on standard contractual clauses for the transfer of personal data to third countries; Commission Decision 2002/16/EC, 2002 O.J. (C) [hereinafter Commission Decision 2002/16/EC], on standard contractual clauses for the transfer of personal data to processors established in third countries.

49. These principles, which essentially mirror the data quality principles as discussed in section II of this article, are set forth, for example, in appendix two (or three) of the Commission Decision of June 15, 2001. *See* Commission Decision 2001/497/EC, *supra* note 48.

50. *Id.* Preamble 5.

51. *Id.*

52. Commission Decision 2002/16/EC, *supra* note 48.

fundamental rights and freedoms of individuals and as regards the exercise of corresponding rights; such safeguards may in particular result from appropriate *contractual clauses*.[53]

The EU felt that two sets of contractual clauses were necessary since Controller to Processor arrangements did not require the same level of safeguards as Controller to Controller—under the former, the controller expressly remains liable vis-à-vis the employee. Specifically, the Commission stated that for Controller to Processor transfers, "[t]he data importer should process the transferred personal data only on behalf of the data exporter and in accordance with his instructions and the obligations contained in the clauses"[54] and that "the contract should be governed by the law of the Member State in which the data exporter is established enabling a third-party beneficiary to enforce a contract."[55] Accordingly, the data exporter remains liable vis-à-vis the employee for the data importer's breach of the standard contractual clause.[56] The data exporter and data importer must determine between themselves which of the standard contractual clauses is appropriate for their particular data transfer.

The Commission's Decision of June 15, 2001, sets forth the second set of EU standard contractual clauses for the transfer of data from an EU controller to a controller outside the EU.[57] Data transfers under Controller to Controller arrangements require different control measures than do Controller to Processor arrangements since, under the former, the data essentially leaves the control of the initial controller. Controller to Controller standard contractual clauses have been the subject of criticism to the point that a number of agencies submitted their own proposed standard contractual clauses with hopes that the Commission would approve them.[58] The providers of these proposed standard contractual clauses argued that existing standard contractual clauses are not commercially realistic in that they do not allow for flexibility and can be overly burdensome.[59] It is for this reason, it is argued, that the standard contractual clauses have gained acceptance almost exclusively between affiliated companies and have not gained acceptance for transactions between independent third parties.[60]

From a content point of view, the four most significant (and often controversial) aspects of the standard contractual clauses, depending on whether the parties are using the Controller to Controller or Controller to Processor clauses, are: (1) third-party beneficiary rights; (2) the parties' obligations; (3) joint and several liability; and (4) governing law.

53. Directive, *supra* note 4, art. 26(2).

54. Commission Decision 2002/16/EC, *supra* note 48, Preamble 14.

55. *Id.* Preamble 18.

56. *Id.* annex clause 3, 6(1).

57. Commission Decision 2001/497/EC, *supra* note 48.

58. The International Chamber of Commerce (ICC), the Federation of European Direct Marketing (FEDMA), the EU Committee of the American Chamber of Commerce in Belgium (Amcham), the Japan Business Council in Europe (JBCE), the Confederation of British Industry (CBI), the International Communications Round Table (ICRT) and the European Information and Communications Technology Industry Association (EICTA) submitted joint proposed standard contractual clauses to the European Commission. International Chamber of Commerce, *Proposed Standard Contractual Clauses for the Transfer of Personal Data from the EU to Third Countries* (Sept. 7, 2001), *available at* http://www.iccwbo.org/home/statements_rules/statements/2001/contractual_clauses_for_transfer.asp.

59. *See* KUNER, *supra* note 19, at 150-52.

60. *Id.* at 150.

Regardless of whether using Controller to Controller clauses or Controller to Processor clauses, the EU expressly authorizes employees to enforce their rights as third-party beneficiaries for particular breaches of the clauses.[61] This ensures that employees, who are supposed to be the actual beneficiaries of these clauses, have a right to compensation for any damages they may suffer as the result of a breach by either the data exporter or data importer.

The obligations of the data exporter and data importer for Controller to Controller arrangements are relatively straightforward. When completing the standard contractual clauses, the parties must devote most of their attention to appendix one, which requires the parties to set forth various matters regarding the proposed transfer, including the purposes of the transfer, descriptions of data they will transfer, whether they will transfer sensitive data, and information regarding storage of the data.[62] One practical issue that almost always arises concerns how specific this information needs to be. Not surprisingly, data authorities prefer very specific responses. Practice has shown, however, that parties invariably include some general remarks when completing appendix one as they want to ensure that the standard contractual clauses cover all of the data they are transferring. For example, the purpose of the data transfer may be for cost-efficiency purposes by listing data at one central location, or the employer may describe the categories of data it will transfer as general employment and personal data. Though employers should make every effort to give specific information when completing appendix one, the reality is that this practice is not always feasible.

The data exporter's obligations under the Controller to Processor arrangements require a different focus than under Controller to Controller arrangements. Under the former, the data exporter must not only instruct the data importer to process the data on behalf of the data exporter and in accordance with its instructions, but the data exporter must also ensure that the data importer has appropriate "technical and organizational security measures"[63] in place, such as encryption software and passwords. Unfortunately, there is no uniform level of technical and organizational security measures among the member states.[64] As a result, in appendix two of the standard contractual clauses, the data importer and data exporter must provide the security measures the data importer will implement. The data exporter represents and warrants (*vis-à-vis* the third-party beneficiary employees) that the data importer will provide sufficient guarantees regarding technical and organizational security measures. Security measures adopted by the data importer will often be the crux of the agreement with the data exporter; nevertheless, as stated above, use of standard contractual clauses is generally not subject to data protection authorities' approval. As a result, the data exporter and importer are essentially forced to rely on their own expertise when determining whether the security measures the data importer will implement are sufficient for EU data protection authorities' purposes.[65]

For many, the most troubling aspect of the clauses is the liability clause as set forth in clause 6 of each standard contractual clause. Under Controller to Processor arrangements,

61. Commission Decision 2001/497/EC, *supra* note 48, cl. 3; Commission Decision 2002/16/EC, *supra* note 48, cl. 3.

62. Commission Decision 2001/497/EC, *supra* note 48, app. 1.

63. Commission Decision 2002/16/EC, *supra* note 48, annex cl. 4(c), app. 2.

64. *See* KUNER, *supra* note 19, at 199-201.

65. *Id.* at 154-55.

a third-party beneficiary employee may recover damages against the data exporter even if the data importer breached one of its specific obligations.[66] The exporter may then seek indemnification from the data importer.[67]

Even more far-reaching is that under the Controller to Controller clauses, the data exporter and data importer are jointly and severally liable for those provisions pursuant to which the employee is a third-party beneficiary.[68] Joint and several liability was one of the more hotly-debated issues between the EU Commission and various lobbying organizations. For example, it was argued by the International Chamber of Commerce (ICC) that joint and several liability as originally presented "is far too broad and undifferentiated."[69] Although the Commission did introduce some changes to the contractual clauses (for example, joint and several liability is limited to clauses in which the employee is a third-party beneficiary), it did retain the concept of joint and several liability, pointing out in its response to the ICC that such liability "will provide strong incentives to the parties to give close attention to each other's compliance with the data protection clauses of the contract, which they might otherwise tend to neglect given that neither party is the direct beneficiary of these clauses."[70] The Commission continued by adding that the liable party can seek indemnification against the breaching party.[71] It goes without saying that not everybody considers this to be an adequate remedy, since, as the ICC aptly pointed out, "joint and several liability is an anomaly in commercial contracts."[72]

Another contractual clause causing concern among data exporters is the governing law clause. Each set of standard contractual clauses requires that the laws of the data exporter's jurisdiction, that is the laws of the state where the employer is located in the EU, govern.[73] Any jurisdictional issues that might arise can become extremely complicated and are beyond the scope of this article.[74]

The second noteworthy aspect of the governing law clause is that it leaves another issue unresolved—specifically, the question whether the standard contractual clauses must be in the form of a bilateral or multilateral agreement. In other words, can a parent corporation

66. Commission Decision 2002/16/EC, *supra* note 48, annex cl. 6(1).

67. *Id.* annex cl. 6(3).

68. *Id.*

69. Letter from Maria Livanos Cattaui, Secretary General, International Chamber of Commerce, to Frits Bolkenstein, Commissioner, European Commission (March 13, 2001) (*available at* http://europa.eu.int/comm/internal_market/privacy/docs/clausexchange/letterice_en.pdf) [hereinafter ICC Letter]. *See also* Letter from Maja Wessels, Chair, EU Committee of the American Chamber of Commerce in Belgium, to Frederick Bolkenstein, Commissioner, European Commission (March 23, 2001) (*available at* http://europa.edu.int/comm/internal_market/privacy/docs/clausexchange/letteracc_en.pdf) [hereinafter ACC Letter].

70. Letter from John F. Mogg, Director General, European Commission, to Maria Livanos Cattaui, International Chamber of Commerce (2001) (*available at* http://europa.edu.int/comm/internal_market/privacy/docs/clausexchange/replyicc_en.pdf).

71. *Id.*

72. ICC Letter, *supra* note 65.

73. Commission Decision 2001/497/EC, *supra* note 48, cl. 10; Commission Decision 2002/16/EC, *supra* note 48, cl. 9.

74. *See* KUNER, *supra* note 19, at 85-116. (discussing the complex jurisdictional issues that often arise in cross-border data transfers). Unfortunately, but not surprisingly, the EU does not provide uniformity on this very important issue since the non-uniform laws of the individual member states will dictate which country or countries have proper jurisdiction over a particular dispute.

conclude a single agreement with all of its subsidiaries, or must each subsidiary conclude an individual agreement with every subsidiary to which it transfers information plus the parent corporation? Needless to say, the latter could turn out to be an administrative nightmare for large, multinational companies because this would require "hundreds, if not thousands" of such agreements.[75] This unresolved issue is a "governing law" issue—if companies are permitted to conclude multilateral agreements, they will, in all likelihood, not be able to satisfy the requirement that the laws of the data exporter's jurisdiction apply to the clauses since exporters will be from various jurisdictions.

Since the EU has not provided a definitive answer to this unresolved question,[76] many companies have taken a rather practical approach by doing a quick risk analysis. In essence, they utilize multilateral agreements, agreements among the parent corporation and several subsidiaries for data that are not at all or less sensitive, making it less likely that an employee will file a complaint, thereby exposing the company to less potential liability. They then take the extra step of utilizing bilateral agreements, agreements between only two entities when processing more sensitive data or when the data are of a type that it is not prudent for each of the other entities to know that the employer is transferring such data.

This analysis, however, is not without risk. Although the data exporter may have a good understanding of the data being transferred, which should be determinable through an audit, the data exporter may still misjudge the sensitivity of particular data as this is a judgment call on the employer's part. For example, companies may elect to classify information by categories such as sensitive data, including whether an employee is disabled or pregnant; confidential data, like the name of a previous employer; and business information data, such as the employee's cell phone number. As a result of this analysis, if an employer legitimately processes data concerning an employee's disability or pregnancy (sensitive data) and then transfers this data outside of the EU using a standard contractual clause, then the data exporter and data importer should conclude a separate bilateral agreement. This same company may then transfer non-sensitive or less sensitive information, such as business information, using a multilateral standard contractual clause for all of the affiliates and the parent corporation.

Engaging in such risk analysis may result in the company violating the letter (and possibly the spirit) of the Commission's Decision, in which case the standard contractual clauses could be voided. Therefore, companies should proceed with caution when following this strategy.

Standard contractual clauses as provided by the Commission are, by their very nature, inflexible. This is one of the loudest complaints regarding these clauses. However, much to the surprise and delight of many, on December 27, 2004, the Commission approved standard Controller to Controller contractual clauses as proposed by seven business asso-

75. Rittweger & Weisse, *supra* note 18, at 142 n. 21.

76. However, the Commission did refer to "standard contractual clauses with many parties to the contract." Article 29-Data Protection Working Document: 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, June 3, 2003 (11639/02/EN WP 74), at 7, *available at* http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2003/wp74_en.pdf [hereinafter Commission Working Document 74].

ciations.[77] These alternative standard contractual clauses[78] permit increased flexibility and address some of the issues discussed above. Parties may begin using the alternative standard contractual clauses as of April 1, 2005.[79]

For example, employees as third-party beneficiaries may not take action against the data importer directly until after they give the data exporter reasonable time (the suggested time is one month) to enforce the clauses against the data importer.[80] In order to give this clause more bite, employees have the right to pursue an action directly against the data exporter if the data exporter failed to undertake reasonable due diligence to ensure itself that the data importer is truly able to satisfy its contractual obligations.[81] Though this alternative puts a greater onus on the data exporter and data importer to engage in reasonable due diligence *prior* to concluding the contractual clauses, it limits an employee's ability to automatically enforce his rights as a third-party beneficiary since it must first give the data exporter a chance to cure the breach. This alternative directly addresses the concern of many companies that the EU's standard contractual clause gives employees the automatic right to seek redress without giving the data exporter and data importer a reasonable opportunity to rectify any breach.

In addition, the alternative standard contractual clauses do not call for joint and several liability. Instead, the data exporter and data importer each are required to engage in reasonable due diligence prior to concluding the contractual clauses.[82] Each party is only subject to liability for damages for which it was responsible.

Another departure from the EU's standard contractual clauses is that, under the alternative standard clauses, data exporters are not required to disclose the full text of the contractual clauses to employees if the contractual clauses include confidential information. Instead, if the data exporter elects to redact some of the information in the contractual clauses, it must inform the requesting employee accordingly and provide the reasons for the action. The employee may ask the data protection authorities to review whether such a redaction of information is justified.[83]

Although, without a doubt, they add flexibility when compared to the Commission's original standard contractual clause, the use of the alternative standard contractual clauses is, for the moment, untested. How the business world will receive them remains to be seen.

Taking all of the above into consideration, the most significant advantage of standard contractual clauses is that they are straightforward and relatively simple to use. Further,

77. Press Release, International Chamber of Commerce, European Union Approves Clauses for International Data Transfers (Jan. 7, 2005) (*available at* http://www.iccwbo.org/home/news_archives/2005/data_transfers.asp) [hereinafter Press Release, International Chamber of Commerce]. *See also*, Press Release, European Commission, Data Protection: Commission Approves New Standard Clauses for Data Transfers to Non-EU Countries (Jan. 7, 2005) (*available at* http://europa.eu.int/rapid/pressReleasesAction.do?reference=IP/05/12&format=HTML&aged=0&language=EN&guiLanguage=en).

78. International Chamber of Commerce Dept. of Policy and Business Practice Task Force on Privacy and the Protection of Personal Data, *Final Approved Version of Alternative Standard Contractual Clauses for the Transfer of Personal Data from the EU to Third Countries (Controller to Controller Transfers)* (Jan. 7, 2005), *available at* http://www.iccwbo.org/home/e_business/ICC_model_clauses_FAQs.pdf.

79. *Id.*

80. Press Release, International Chamber of Commerce, *supra* note 77, cl. III(b).

81. *Id.*

82. *Id.* cl.s I(b), II(f).

83. *Id.* cl. I(e).

their use provides adequate data protection as required by article 26 of the Directive.[84] Unlike self-certification under Safe Harbor,[85] the parties do not need to make their contractual clauses public. Instead, they are private agreements between the signatories with the understanding that they provide certain third-party beneficiary rights. Finally, data protection authorities do not need to approve their use.[86] In essence, the standard contracts serve as a ready and relatively inexpensive form of data protection agreement that permits employers to transfer data from the EU to any corner of the world. Experience has shown that, while standard contractual clauses are far from perfect, they may be useful to affiliated companies to whom the Safe Harbor Agreement described below is either unavailable, impractical, or simply undesirable.

2. *Self-Certification under Safe Harbor*

Another alternative available for companies to legally transfer data from the EU is for the U.S. recipient of that data to become self-certified under the Safe Harbor Agreement as negotiated by the United States and the EU.[87] The Safe Harbor, however, applies only to data transfers from the EU to the United States. Also, the Safe Harbor is limited only to those companies that the Federal Trade Commission (FTC) or the Department of Transportation (DOT) regulates.[88]

84. Commission Decision 2002/16/EC, *supra* note 48, art. 1, pg 52; Commission Decision 2001/497/EC, *supra* note 48, art. 1, pg 19.

85. *See* infra section III.A.2.

86. However, the national data protection authorities may require the parties to deposit the standard contractual clauses. Commission Decision 2002/16/EC, *supra*, note 48, cl. 8(1), pg 59 (concerning transfer of personal data to processors established in third countries); Commission Decision 2001/497/EC, *supra* note 48, cl. 8, pg 26 (concerning the transfer of personal data to third countries.). *See, e.g.*, KUNER, *supra* note 19, at 149-50, in which it is stated that

> [i]n some member states (for example, the Netherlands) transfers under the clauses must still be notified to, and possibly also authorized by, the national [data protection authorities] before the transfer is made, though such notification should in practice be little more than a formality as long as the clauses are properly used.

The use of standard contractual clauses as provided by the Commission may not suffice for Spanish law purposes since, pursuant to Rule 5(2) of Instruction 1/2000 of December 1, 2000, the Spanish Director of the Data Protection Agency may still need to authorize the data transfer, BOE 201, December 16, 2000. If the transfer is subject to an authorization, the data protection agency will only grant such an authorization if the employer submits a written contract setting forth those points listed in Rule 5(2) of Instruction 1/2000. These points resemble the principles of the standard contractual clauses in many respects, but are also more onerous in a few respects, e.g., the parties must provide that not only will they be jointly and severally liable vis-à-vis the employees, but also vis-à-vis the Spanish Data Protection Agency and Spanish legal authorities. Norma quinta, Instruccion 1/2000 de la Agencia de Proteccion de Datos (B.O.E., 2000, 301), *available at* http://www.boe.es/bue/dias/2000-12-16/pdfs/A44253-44257.pdf.

87. Commission Decision 2000/520/EC, 2000 O.J. (L 215) 7; Notice from Department of Commerce—International Trade Administration, 65 Fed. Reg. 45,666 (July 24, 2000) [hereinafter Notice 45,666].

88. Any U.S. organization that is subject to the jurisdiction of the Federal Trade Commission (FTC) or U.S. air carriers and ticket agents subject to the jurisdiction of the Department of Transportation (DoT) may participate in the safe harbor. The Federal Trade Commission and the Department of Transportation have both stated in letters to the European Commission that they will take enforcement action against organizations that state that they are in compliance with the Safe Harbor framework but then fail to live up to their statements . . .

U.S. Department of Commerce, Safe Harbor Workbook, *at* http://www.export.gov/safeharbor/sh_workbook.html (last visited Feb. 21, 2005). Businesses operating in the financial services or insurance sectors are the two primary exceptions to companies that may become self-certified under the Safe Harbor. *Id.*

Since November 2000, the EU Commission and the U.S. federal government have had in place the Safe Harbor Arrangement, which permits EU companies to process and transfer EU personal data to the United States.[89] Safe Harbor registrants must place strict limitations on the transfer of personal data, verify such data, and certify to the U.S. Department of Commerce or the DOT (whichever the case may be) that they are in compliance with the Safe Harbor Agreement. They must also agree to be subject to certain enforcement measures, including dispute resolution for EU employees whose data is being collected.

In order to qualify for the Safe Harbor, the registrant must agree to observe certain principles. Not surprisingly, these Safe Harbor principles essentially mirror those found in the Directive. As a result, this article only briefly lists those principles. They are as follows:[90]

1) Notice: The employer must clearly inform its employees what personal information is being collected, why this information is being collected, how it plans to use such information, who the employee can contact with inquiries and complaints, the third parties to whom the employer may disclose the employee data, and how the employee can restrict the use and disclosure of such information (preferably by including a statement in an attachment to the employment agreement or, if applicable, in a works agreement).
2) Choice: The employer must present the employee with a meaningful opt-out choice if the employer intends to disclose the data to a third party or use it for a purpose not previously authorized. The exercise of this opt-out choice must be free from any negative ramifications on the employee for so choosing. For "sensitive data," the employer must provide an explicit opt-in procedure.
3) Limitations on Onward Transfers: To transfer data to third parties, employers must observe the above "Notice" and "Choice" principles. Additionally, employers must limit the disclosure of employee personal data to a third party that has agreed to adhere to the Safe Harbor principles, is subject to the Directive, or otherwise satisfies the "adequate protection" standard.
4) Security: The employer must provide reasonable security measures to ensure that employee personal data is protected from loss, destruction, misuse, unauthorized access, etc.
5) Assurances of Data Integrity: Any personal information collected must be relevant to the purposes for which it is to be used. The employer may not process data beyond what has been previously authorized and must take reasonable precautions to ensure that collected data is accurate, complete, and up to date.
6) Access: Employers must grant the respective employees reasonable access to the information they store regarding such employees, weighed against concerns for the rights of other persons whose interests may be violated through such actions. In addition, employers must give employees an opportunity to correct, amend, or delete any inaccuracies.
7) Effective Enforcement Mechanism: The employer must provide an independent, readily available, and affordable dispute resolution mechanism for investigating and

89. *See generally*, U.S. Department of Commerce, Welcome to the Safe Harbor, *at* http://www.export.gov/safeharbor/index.html (last visited Feb. 21, 2005). As of April 13, 2005, 699 companies were self-certified under the Safe Harbor Arrangement. *Id.*

90. *Id.*

resolving employee complaints and disputes over the collection and processing of their personal data. Employers must also put into place a procedure for independently verifying compliance with the Safe Harbor principles.

The following aspects comprise an effective enforcement mechanism: verification, dispute resolution, and remedies. Verification requires most companies to audit their data processing policies and practices to evaluate whether any corrective steps are needed in order to comply with the Safe Harbor principles. Depending on the findings, this may be a daunting task. Also, and not to be underestimated, an employee's right to be informed about the purpose and scope of the data processing and the ability to limit exposure of such data to third parties may force employers to make extensive, and possibly costly, changes to their data handling procedures.

The company can conduct the audit itself or it may hire an independent third party to perform the audit.[91] Included as part of the audit are determinations as to: (1) which databases include information about employees in the EU; (2) what information the employer is transferring from the EU to the United States and how much of this information the employer actually needs to transfer; (3) what data an employer is making available to third parties (including affiliated companies); and (4) what sensitive data the employer is transferring.

Whether the company needs to introduce any corrective measures depends on the results of the audit. One of the fundamental errors that companies too often make is to underestimate the importance of a comprehensive audit. In order to be effective, an audit should have the approval and support of management, and it should create an accurate picture of what data are actually being transferred and to what databases particular individuals have access. The final step of the verification process is to include a statement in the company's privacy policy that its privacy policy conforms to the Safe Harbor principles.

The second and third aspects of enforcement under the Safe Harbor, dispute resolution and remedies, are related. In order to comply with the Safe Harbor principles, companies may join a private sector-developed privacy program that includes effective enforcement mechanisms, such as TRUSTe, Judicial Arbitration and Mediation Service (JAMS), the American Arbitration Association, or BBBOnline seal program.[92] A company should take care in selecting an appropriate regime because, according to the Commission, even though there is "little experience on which to determine whether the [dispute resolution regimes]

91. Notice 45,666, *supra* note 87, at 45,670 (FAQ 7—Verification). According to this Department of Commerce Notice, "the FAQs [ ] are intended to serve as *authoritative guidance* to U.S. companies and other organizations receiving personal data from the European Union and wishing to establish a predictable basis for the continuation of such transfers." *Id.* at 45, 666. As a result, it is imperative that U.S. companies acquaint themselves with the FAQs if becoming self-certified under the Safe Harbor.

92. *See* Commission Staff Working Paper: The Application of Commission Decision 520/2000/EC of 26 July 2000, pursuant to Directive 95/46 of the European Parliament and the Council on the Adequate Protection of Personal Data Provided by the Safe Harbour Privacy Principles and Related Frequently Asked Questions Issued by the Department of Commerce, Feb. 13, 2002 (SEC(2002)196), at 7, *available at* http://europa.eu.int/comm/internal_market/privacy/docs/adequacy/sec-2002-196/sec-2002-196_en.pdf [hereinafter Application of Commission Decision 520/2000/EC]. Neither the Department of Commerce nor the Department of Transportation certifies these programs; instead, the company self-certifying must ensure that the dispute resolution provider it has chosen satisfies the Safe Harbor provisions. Notice 45,666, *supra* note 87, at 45,673 (FAQ 11—Dispute Resolution and Enforcement).

carry out their roles properly,"[93] the Commission has "detected some failures" with respect to the transparency of these bodies and their sanctioning practices.[94]

In the alternative, a company may commit to cooperating with European data protection authorities.[95] If a company transfers human resources data from the EU to the United States under the Safe Harbor Arrangement, however, it does not have a choice between a private-sector dispute resolution regime or EU data protection authorities; instead, the Safe Harbor Agreement requires the company to cooperate with the EU data protection authorities[96] with respect to the transfer of human resources data. An absence of this requirement would place European employees in the unenviable position of having to seek a remedy in the United States. In essence, if the EU had not insisted on this concession from the United States, the U.S. party would not have had to give any serious thought to whether it was violating the Safe Harbor principles, because the likelihood that an EU-based employee would seek redress in the United States would have been minimal.

The final aspect of enforcement is remedial measures. To date, the EU authorizes only the FTC and the DOT to investigate complaints and to impose sanctions.[97] The authorization of each of these bodies is based on its authority to determine whether companies subject to these agencies' jurisdiction have engaged in an unfair and deceptive practice.[98] If a company states that it is self-certified under Safe Harbor but does not comply with the principles or otherwise violates the Safe Harbor Arrangement, then it is guilty of engaging in an unfair and deceptive practice.[99] Since no company has been pursued for non-compliance of the Safe Harbor principles yet, it is fair to say that the chances of the FTC or DOT acting on their own initiative in the near future are limited. In fact, according to Professor Joel Reidenberg of Fordham University,[100] one of the authors of a recent Safe Harbor study

93. Commission Staff Working Document: The Implementation of Commission Decision 520/2000/EC on the Adequacy Protection of Personal Data Provided by the Safe Harbour Privacy Principles and Related Frequently Asked Questions issued by the U.S. Department of Commerce, Oct. 20, 2004, (SEC (2004) 1323, at 11, *available at* http://europa.eu.int/comm/internal_market/privacy/docs/adequacy/sec-2004-1323_en.pdf [hereinafter Implementation of Commission Decision 520/2000/EC].

94. *Id.*

95. Notice 45,666, *supra* note 87, at 45,669 (FAQ 5—The Role of the Data Protection Authorities).

96. *Id.* at 45,672-73 (FAQ 9—Human Resources).

97. *Id.* annex list, of U.S. Statutory Bodies Recognized by the European Union at 45668.

98. U.S.C. §45 (2004); 49 U.S.C. §41712. However, there has been some debate as to whether the FTC's jurisdiction is qualified for employment-related data despite the FTC's assertion in 1998 that the FTC has "carefully reviewed the FTC authorizing legislation, related documents, and relevant case-law and [has] concluded that the FTC has the same jurisdiction in the employment-related data situation as it would generally under Section 5 of the FTC Act." Letter from Robert Pitofsky, FTC Chairman, to John F. Mogg, Director General, European Commission (July 14, 200), *available at* http://www.useu.be/ISSUES/ftc0714.html. Further, the FTC confirmed that the

> FTC will bring privacy-related enforcement actions in situations involving data transfers between companies . . . [The FTC] expect[s] this situation is the one in which the employment issue is most likely to arise, as employment data about Europeans is transferred from European companies to American companies that have pledged to abide by the safe harbor principles.

Id. Nevertheless, "there is no evidence that the FTC or DoT has undertaken enforcement actions" to date. Safe Harbour Decision Implementation Study, (April 19, 2004), at 21, *available at* http://europa.eu.int/comm/internal_market/privacy/docs/studies/safe-harbour-2004_en.pdf [hereinafter Safe Harbor Implementation Study]. *See also, id.* (discussing the FTC's jurisdiction).

99. 15 U.S.C. §45;49 U.S.C. §41712.

100. Alan Pedersen, *U.S. Safe Harbor Under Fire*, 75 Privacy Laws & Business 3 (October/November 2004), at http://www.privacylaws.com/pdfs/newsletters/intnews75.pdf;

assigned by the Commission, "[o]ne gains an impression that US authorities—particularly the FTC—are not especially interested in Safe Harbor implementation and enforcement."[101]

If the FTC should find that a company is violating section five of the FTC Act, the FTC may either seek a cease and desist order that prohibits the company from claiming it is complying with the Safe Harbor or file a complaint in federal court.[102] The FTC also has the authority to impose a civil penalty if the company does not observe a cease and desist order and may pursue civil or criminal charges for violation of a court order.[103] The FTC would then notify the Department of Commerce of its findings. A persistent failure to abide by the Safe Harbor is actionable under the False Statements Act.[104] Similarly, the DOT has the authority to order companies under its jurisdiction to cease from engaging in an unfair and deceptive practice.[105]

Becoming self-certified under the Safe Harbor is strictly voluntary and offers some distinct benefits. Undoubtedly, the most significant benefit is that self-certification under the Safe Harbor includes a presumption of adequate protection for data transfers from the EU to the United States. Just as important for many U.S. companies is the fact that U.S. law governs such data transfers and a U.S. agency or U.S. arbitral body rules upon it; except, of course if the company agrees to cooperate with EU data protection authorities, either because it is required to do so when human resources data is involved or because it voluntarily agreed to cooperate.[106]

Why would a company voluntarily opt to cooperate with EU data protection authorities? Experience has shown that this is primarily for cost reasons. The fees of the private sector bodies mentioned above are generally much higher than the European data protection authorities' fees.[107]

Regardless, the fact that U.S. law usually governs data transfers and that a U.S. body will render decisions gives many American companies added comfort, making the Safe Harbor more attractive to them. An additional benefit is that the actual self-certification process is straightforward, a party can complete the forms available on the Department of Commerce website relatively quickly.[108]

101. Safe Harbor Decision Implementation Study, *supra* note 98.

102. Notice 45,666, *supra* note 87, at 45,673-74 (FAQ 11—Dispute Resolution and Enforcement).

103. *Id.*

104. 18 U.S.C. §1001 (2004).

105. 49 U.S.C. §41712.

106. However, even if the company stated that it would not cooperate with the EU data protection authorities, companies should be aware that the risk remains that an EU data protection authority will take jurisdiction of an infringement—if the alleged infringement was carried out within the EU or if the data processor is subject to the laws of an EU jurisdiction. See, e.g., Articulo 2, Ley Organica 15/1999, de Proteccion de Datos de Caracter Personal (B.O.E. 1999, 298).

107. The EU data protection authorities charge on the basis of the company's revenues. As of the time of this writing, the EU data protection authorities charged U.S. $150 per year for companies with annual revenues of less than U.S. $25 million, U.S. $300 per year for companies with annual revenues of between U.S. $25 million and U.S. $100 million, and U.S. $500 per year for companies with annual revenues in excess of U.S. $100 million. U.S. Department of Commerce, Welcome to the Safe Harbor, *at* http://www.export.gov/safeharbor/index.html (last visited Mar. 4, 2005).

108. Companies can become self-certified by filling out the form available for review at Certifying an Organization's Adherence to the Safe Harbor, *available at* http://www.privacyassociation.org/docs/sum04/5Rohlmeier3.pdf (last visited Mar. 4, 2005).

As discussed above, one step in the self-certification procedure is for the company to include that it has become self-certified in its published privacy statement.[109] The company must also indicate in its privacy policy whether the verification is done in-house or whether it has engaged a third party. The company must self-certify on an annual basis. Although the company is permitted to withdraw at any time, it remains liable for any violations that occurred during the period of self-certification.

Another practical consideration for companies deciding whether to become self-certified under the Safe Harbor is that an employer can use the Safe Harbor only for data transfers from the EU to the United States, not for data transfers to any other country. This distinguishes the Safe Harbor from the standard contractual clauses, as an employer can use the latter for the transfer of data to any country. Since, for logistical reasons, companies generally seek to have a uniform data transfer mechanism in place, the Safe Harbor is not conducive for many multinationals since it forces these companies to rely on additional approved schemes, such as standard contractual clauses or codes of conduct, for the transfer of the same or similar information to countries other than the United States.

Since its inception, approximately ten to twenty-five U.S. companies per month have become self-certified under the Safe Harbor per month. The reluctance of many U.S. companies to sign onto the Safe Harbor Agreement is due in part to "fear of the unknown," but is also due to companies not wanting to expose themselves to additional potential liability, as well as companies' general reluctance to make information public. Some may argue, however, that the public nature of the Safe Harbor could serve as a motivating factor for companies, considering that part of the Safe Harbor Arrangement is a public statement that particular data privacy principles are being observed. Companies whose data privacy policies have been questioned might try to use self-certification, in part, as a public relations tool.[110] By making a public statement that the company has in place a strict data privacy policy as published by the U.S. government, companies may receive some positive publicity.[111]

Still, the EU is not satisfied with the relatively low number of companies that have become self-certified under the Safe Harbor Agreement.[112] Many problems were attributed

109. Notice 45,666, *supra* note 87, at 45,669-70 (FAQ 6—Self-Certification).The Commission found that a number of companies do not include such a statement in their privacy policies, and thus, they are in violation of FAQ 6. Further, some companies have chosen to become self-certified under the Safe Harbor only for the purpose of transferring human resources data from the EU to the United States. Many of these companies do not include a corresponding statement in their privacy policies, but instead, since it concerns only employees, have made this known only through the use of employee manuals or though an intranet page. Application of Commission Decision 520/2000/EC, *supra* note 92, at 8. Whether such a limited disclosure truly satisfies the requirements of FAQ 6 remains to be seen.

110. *See, e.g.*, Press Release, FTC, Microsoft Settles FTC Charges Alleging False Security and Privacy Promises (Aug. 8, 2002), *at* http://www.ftc.gov/opa/2002/08/microsoft.htm; Joseph Menn, *Security Flaws May be Pitfall for Microsoft*, L.A. Times (Jan.14, 2002) at C1; Jonathan Krim, *Microsoft's One-ID Plan Again Draws Fire Over Privacy*, Wash. Post (Aug. 16, 2001) at E1; Steve Lohr, *Privacy Group is Taking Issue with Microsoft*, N.Y. Times (July 25, 2001) at C1.

111. *See, e.g.*, *Helping Protect Privacy at Microsoft* (Nov. 13, 2002), at http:// www.microsoft.com/security/articles/safe_harbor.asp (confirming that Microsoft is a "participant in the Safe Harbor Agreement between the United States and the European Union, and [that Microsoft] meets the Safe Harbor principles published by the U.S. Department of Commerce").

112. "The number of companies to have self-certified and that can therefore be assured of the benefits of the Safe Harbor is lower than expected . . ." Application of Commission Decision 520/2000/EC, *supra* note 92, at 5 (commenting on the fact that only 129 companies had become self-certified as of December 1, 2001).

to "teething problems" caused by the Safe Harbor's relative infancy.[113] Despite the low number of self-certified companies, several large multinational companies decided to go forward with the Safe Harbor self-certification process.[114] Companies will continue to see the benefits of becoming self-certified under the Safe Harbor for the next few years, but it appears likely that as Codes of Conduct (see section three, below) become more publicized and more popular and data protection authorities devote greater resources to their enforcement policies, the Safe Harbor will remain attractive primarily to only smaller and medium-sized enterprises (SME). Thus, it is likely that fewer large and multinational entities will see the Safe Harbor Arrangement as a satisfactory alternative for transferring data to the United States. Instead, it is probable that many will complete a risk/benefit analysis and conclude that risks, such as additional potential liability for breach of section five of the FTC Act and the public disclosure of data privacy policies that essentially "invites" parties to file claims, will outweigh the benefits, primarily the ability to transfer data from the EU to only the United States.

3. *Codes of Conduct*

Compared to the standard contractual clauses and the Safe Harbor, Codes of Conduct are the "new kids on the block." As already stated in section III.A.1, article 26(2) of the Directive states that the adequacy of "safeguards may *in particular* result from appropriate contractual clauses."[115] Since the Directive uses the wording "in particular," this means that other alternatives are available to meet the adequate protection test. One such alternative is quickly gaining popularity: the so-called Code of Conduct. Codes of Conduct will, undoubtedly, become even more popular following article 29's publication of a Working Document regarding Codes of Conduct.[116] The Working Party that produced the Working Document refers to the Codes as "binding corporate rules for international data transfers" or "legally enforceable corporate rules for international data transfers."[117]

Company Codes of Conduct, however, are not a panacea for the transfer of data to all parties throughout the world. Company-level Codes of Conduct are prepared at the company level and, therefore, apply only at that level. Thus, as reiterated throughout the article 29 Working Document, companies use Codes of Conduct almost exclusively for the transfer of information to members within a corporate group. For example, DaimlerChrysler AG

Further, "the number of registered organisations is lower than initially anticipated and this is a cause of disappointment for the Commission services insofar as the benefits of the Safe Harbour would be greater (both for companies and for data subjects) if membership were to increase further." Implementation of Commission Decision 520/2000/EC, *supra* note 93, at 5 (commenting that 401 companies had become self-certified as of November 3, 2003).

113. Application of Commission Decision 520/2000/EC, *supra* note 92, at 11.

114. For example, Microsoft, Eastman Kodak Company, General Motors Corporation, Goodrich Corporation, Hewlett-Packard, IBM, Intel, Northrop Grumman Corporation, Oracle Corporation, Procter & Gamble and Wm. Wrigley Jr. Company have all become self-certified.

115. Council Directive 95/46, art. 26(2), 1995 O.J. (L281) 46.

116. Commission Working Document 74, *supra* note 76.

117. *Id.* at 8. *See also Task Force on Privacy and Protection of Personal Data, Int'l Chamber of Commerce*, ICC Report of Binding Corporate Rules for International Transfers of Personal Data 5-7 (Oct. 28, 2004), *available at* http://www.iccwbo.org/home/e_business/FINAL%20ICC%20BCRs%20report%20rev.pdf. (discussing the differences between Codes of Conduct and Binding Corporate Rules).

issued two Codes of Conduct, one pertaining to customer/supplier data[118] and the other concerning employee-related data.[119]

The Code of Conduct prohibits the onward transfer or export of data to non-EU based third parties that are not subject to the Code's provisions, as the receiving party is not subject to the terms of that company's Code of Conduct.[120] Employers must base any such onward transfer on other approved measures, such as standard contractual clauses, Safe Harbor, unambiguous consent from employees, and the like.[121]

One of the primary benefits of corporate Codes of Conduct is that, although data transfers are still subject to approval by data protection authorities, corporations prepare the Codes of Conduct themselves. While Codes of Conduct must reflect the principles set forth above, corporations tend to push the envelope by implementing watered-down versions of other approved measures that serve as their Codes of Conduct.[122]

As mentioned above, the article 29 Working Party prefers referring to the Codes of Conduct as "*binding* corporate rules" or "*legally enforceable* corporate rules for international data transfers."[123] These preferred terms stem from the fundamental requirement that Codes of Conduct must be "binding" on, or "legally enforceable" against, all entities subject to the Code of Conduct, meaning this binding effect will not be limited to within the EU.[124] Instead, the Code of Conduct must be binding on any entity in any country in which it is to apply.[125]

While proof requirements vary by jurisdiction, the Commission leaves to the company's discretion the task of showing the authorizing body that the Code of Conduct is truly binding and legally enforceable. At a minimum, the board of directors or comparable body of the group's parent company, should adopt the Code of Conduct.[126] For example, members of DaimlerChrysler's Board of Management included a statement in each of DaimlerChrysler's Codes of Conduct that it requires all employees to observe the Code's terms and conditions.[127] Further, the company must make certain that all necessary steps have been taken to ensure that the Code of Conduct is not only binding in all those jurisdictions in which it is to apply, but also that it is observed in practice.[128] The Commission sets forth in its Working Paper a number of suggestions designed to "guarantee[ ] a good level of

118. DaimlerChrysler, at http://www.daimlerchrysler.com (last visited Mar. 5, 2005).

119. Though not publicly available, reference is made to it on DaimlerChrysler's home page. *See id.*

120. Commission Working Document 74, *supra* note 76, at 9-10.

121. *Id.* at 9.

122. *See, e.g.*, Hans-Werner Moritz, *Die DaimlerChrysler Codes of Conduct—Der Königsweg?*, TELE-KOMMUNIKATIONS & MEDIENRECHT, at 233 n. 23 (2003) (noting that DaimlerChrysler's Supplier/Customer Code of Conduct does not include a liability clause like is found in the standard contractual clauses).

123. *See* Commission Working Document 74, *supra* note 76.

124. *Id.*

125. *Id.*

126. *Id.* at n. 8.

127. DaimlerChrysler, *Data Protection and Privacy—The DaimlerChrysler Code of Conduct for Customers/Suppliers, available at* http://www.daimlerchrysler.com/Projects/c2c/channel/documents/184265_coc_itr_e.pdf [hereinafter DaimlerChrysler Code of Conduct] (stating, "As an employee of DaimlerChrysler AG or one of its affiliated companies, you are obliged to comply with the principles prescribed by the [Code of Conduct] at work. This will aid in ensuring that our company, our products and our services retain their outstanding image."). *See also* Moritz, *supra* note 122, at 231 (stating the identical statement in DaimlerChrysler's Human Resources Code of Conduct).

128. Commission Working Document 74, *supra* note 76, at 16.

compliance"[129] most notably, but not limited to, audits, education, sanctions, and training programs.

In addition to the binding nature of a Code of Conduct, a company must also provide for adequate enforcement of its provisions. Though the Working Document does not specify the means by which a company is to enforce Codes of Conduct, companies should make employees third-party beneficiaries under a Code of Conduct, as in standard contractual clauses.[130] The Working Document makes clear that employees must have a remedy available if there is a breach of the Code of Conduct. The remedy may either be available under law or by contract.[131] If the only available remedy is under a unilateral Code of Conduct, the employer must ensure that employees can enforce their rights as contractual third-party beneficiaries.[132] The Working Document states that the scope of third-party beneficiary rights in Codes of Conduct "should match at least" such rights as are set forth in the Controller to Controller EU standard contractual clauses.[133]

Although the content of a typical Code of Conduct is beyond the intended scope of this article, it is clear that a company's Code of Conduct must be sufficiently detailed so that its users, third-party beneficiaries, and data protection authorities have an adequate understanding of what information is subject to the Code of Conduct, as well as whether, and under what conditions, the company may transfer such information. With this in mind, Codes of Conduct typically include at least: (1) the company's principles regarding its data privacy policies, which must essentially mirror the principles of standard contractual clauses; (2) employees' rights with respect to the transfer of data concerning such employees; (3) a third-party beneficiary clause; (4) the conditions under which a company may transfer data to parties not covered by the Code of Conduct (so-called "onward transfers"); (5) available remedies for non-compliance; and (6) contact information of the data protection officers.[134] Ultimately, the company determines what information it actually includes and how it tailors its Code of Conduct to meet the goals of the EU and the company. Returning to DaimlerChrysler's Code of Conduct, it is interesting to note that it does not include a liability section.[135] Liability sections typically provide that when a violation of the Code of Conduct occurs, the damaged party is entitled to compensation.[136] This implies that DaimlerChrysler hoped to avoid "inviting" liability claims by not expressly including such a clause in its Code of Conduct.

An important point for this discussion is the issue of jurisdiction. In particular, if the Code of Conduct is breached, in which jurisdiction(s) may a harmed employee seek remedial measures? As mentioned above, the Code of Conduct should set forth any available administrative remedies. If, for whatever reason, these are not sufficient or do not properly address the damages suffered, the employee has the choice of seeking redress in one of two jurisdictions.[137] The employee may file an action against the company in the jurisdiction of

129. *Id.* at 16-17.
130. *Id.* at 12.
131. *Id.* at 11 *et. seq.*
132. *Id.* at 12.
133. *Id.*
134. *See generally id.*
135. *See* Moritz, *supra* note 122.
136. *Id.* at n. 23.
137. Commission Working Document 74, *supra* note 76.

the member in which the "origin of transfer" took place, in the employer's European headquarters jurisdiction, or if different, in the European jurisdiction of the member with delegated data protection responsibilities.[138] It is important to note, however, that these alternatives are limited only to those cases in which the data originated in the EU.

If the data originated outside the EU, then a properly drafted Code of Conduct will *not* allow an employee outside the EU to benefit from the laws of an EU jurisdiction. For example, if a Spanish enterprise has subsidiaries throughout the world and its Guatemalan subsidiary transfers data regarding one of its employees to an affiliated company in Venezuela, the Guatemalan employee is not able to enjoy the protection of Spain's data privacy laws, even if the Spanish, Venezuelan, and Guatemalan entities are each covered by the Code of Conduct. Despite the requisite third party beneficiary clause, a properly drafted Code of Conduct is limited to data originally transferred from the EU and clearly sets forth that the laws of the jurisdiction in which the data originated will apply.[139] Thus, in our example, the employee may seek redress either under Guatemalan or Venezuelan data privacy laws to the extent they exist, but not under Spanish data privacy laws.

Once a company prepares its Code of Conduct, a data transfer or set of data transfers under that particular Code of Conduct may still be subject to the data protection authorities' approval.[140] The remaining question, however, is which data protection authority is the approving body, as there is no such authority at the EU level, including the article 29 Working Party.[141] Accordingly, we must look to the national level since the approving bodies are left to the discretion of the member states. In many EU states, such as Belgium and France, there is only one centralized data privacy authority, which simplifies matters greatly. However, in other states, such as Germany, data protection authorities are at the state level, meaning there may be different data protection authorities within one country.[142] In Germany, this creates serious practical problems because these bodies do not always uniformly apply or interpret Germany's Federal Data Protection Act.[143]

Considering once again DaimlerChrysler, the company requested that data protection authorities of the state of Baden-Württemberg, the German state in which DaimlerChrysler AG has its world headquarters, and the state of Berlin approve a certain set of data transfers.[144] The Baden-Württemberg data protection authorities neither approved nor rejected

138. *Id.* at 19.

139. *See, e.g.*, DaimlerChrysler Code of Conduct, *supra* note 127, art. III (entitled "Application of the Law of Individual Nations").

140. Directive, *supra* note 4, art. 26(2). Depending on the jurisdiction, the Code of Conduct itself may not be subject to approval; instead, the Code of Code may be submitted as part of the request to transfer data to demonstrate to the data protection authorities that steps have been taken to provide adequate protection. *Id.* In some countries, for example Spain, the parties must register the Code of Conduct. Spain Organic Law 15/1999, *supra* note 22.

141. *See supra*, note 19.

142. German Federal Data Protection Act, *supra* note 17, §38(6).

143. Since it is up to the legislators of the sixteen individual German states to delegate the respective data protection authority within that state, the governing bodies among the states are not even uniform. Some states, such as Baden-Württemberg and the Saarland, have delegated this authority to the State Department of Interior, other states, such as Bavaria, Saxony, and Hesse, have delegated it to the Government Administration District, while others, such as Berlin, Bremen, and Hamburg, have delegated it to the State Data Protection Authority, and in Schleswig-Holstein it has been delegated to the Independent State Center. GOLA & SCHOMERUS, *supra* note 17, at 700.

144. *See* Moritz, *supra* note 122, at 229.

DaimlerChrysler's transfer request. Instead, citing Germany's Federal Data Protection Act, the Baden-Württemberg data protection authorities merely opined that DaimlerChrysler's Code of Conduct provided for an adequate level of protection for transfers of data but stated that "responsibility for the admissibility of the transfer shall rest with the body transferring the data."[145] Somewhat differently, the Berlin data protection authorities approved DaimlerChrysler's transfer request.[146] Thus, we clearly have a frustrating predicament: not even the data protection authorities within *one country* treat the export of data under Codes of Conduct uniformly. Further, the various data protection authorities of the twenty-five EU countries do not have uniform laws.

This definitely leaves companies contemplating whether to use a Code of Conduct in a quandary. One point is clear: the fact that one state or regional data protection authority approves a data transfer under a Code of Conduct, which in DaimlerChrysler's case is Berlin, does not mean that other EU members have approved such transfer. There is still no mutuality of recognition within the EU.[147] Instead, at least theoretically, the Code of Conduct user must obtain approval for each transfer of personal data from each data protection authority within the EU, either at the national or regional level. This is theoretical because to expect a company to obtain the approval of every single data protection authority in the EU is simply not realistic. Instead, companies currently need to consider whether they are willing to undertake some risk when enacting Codes of Conduct. There is no evidence that any entity has gone through the unrealistic procedure of having each data protection authority approve transfers of data when using Codes of Conduct.

It seems that Codes of Conduct have the brightest future among the current alternatives available for the transfer of data to countries lacking adequate protection under the EU laws. The increasing popularity of Codes of Conduct pressures the EU Commission to address some very real issues, most notably the absence of any mutual recognition among the member states.

4. *Exemptions under Article 26 of the Directive*

In addition to the methods of transferring data discussed previously, article 26(1) of the Directive states that companies may also transfer data to non-EU countries lacking adequate protection for personal data if the employee consents or if such transfer is "necessary."[148]

145. *Id.* at 229 (citing German Federal Data Protection Act, *supra* note 17, §4b(5)).

146. *Id.*, at 223.

147. However, the EU does promote the cooperation of the various data protection authorities. Commission Working Document 74, *supra* note 76, at 20. Regardless, this cooperation among the EU data protection authorities is not yet sufficient from a practical perspective. In fact, it appears as if there is only one case so far where a member state's data protection authority was assigned to coordinate the approval of a Code of Conduct among all EU member states. On May 28, 2004, the CNIL, France's data protection authority, was assigned the responsibility of coordinating the approval of DaimlerChrysler's Codes of Conduct among all of the EU member states. Professor Dr. Alfred Büllesbach, Presentation at the 26th International Conference on Privacy and Personal Data Protection, (Sept. 16, 2004), at http://26konferencja.giodo.gov.pl/resources/BüllesbachA_pres_en_pdf.

148. Article 26(1) of the Directive states that

> [b]y way of derogation from Article 25 and save where otherwise provided by domestic law governing particular cases, Member States shall provide that a transfer or a set of transfers of personal data to a

The purpose of article 26(1) is to "ensure" that data privacy laws do not unreasonably restrict commercial trade vis-à-vis non-EU countries.[149]

Pursuant to article 26(1)(a), an employer may transfer data to countries not providing adequate protection if the employee has unambiguously given consent. However, as discussed above with respect to the processing of data,[150] employers should treat employee consents with caution. Further, the EU does not subscribe to the argument that an employee has automatically consented to a right to privacy intrusion merely because the matter at issue is work related.[151] Employee consents, whether valid or invalid, probably remain the most common tool used by employers to transfer data.

Companies should consider taking a multi-faceted approach to compliance. Since there is so much uncertainty in the field of data privacy, including questions regarding consent, it is preferable to have more than one accepted compliance method in place rather than to rely exclusively on an employee's consent, especially in the employment context.

The wording of a consent and the purpose given for transferring data is critical. For example, a signed statement by an employee that it consents to the employer's transferring information for any reason the employer sees fit is too vague. The employer must tell the employee the purpose for the data transfer. Further, the employer may not hide the consent in the fine print. Instead, as discussed in section II with respect to consents for data processing under article 7, the consent must be conspicuous, meaning the consent should, at minimum, be a separate document. For all of the reasons mentioned above, employers are ill advised to rely solely on employee consents as a compliance policy.

---

third country which does not ensure an adequate level of protection within the meaning of Article 25(2) may take place on condition that:

(a) the data subject has given his consent unambiguously to the proposed transfer; or
(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject's request; or
(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or
(d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims; or
(e) the transfer is necessary in order to protect the vital interests of the data subject; or
(f) the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case.

Directive, *supra* note 4, at 46.

149. Michael Wächter, DATENSCHUTZ IM UNTERNEHMEN 93 (3d. ed. 2003).

150. See *supra* section II.

151. *See* Halford v. United Kingdom, App. No. 20605/92, 24 Eur. H.R. Rep. 523 (1997) (stating that a right to privacy also extends to the workplace). This holding is similar to a 1987 decision of the U.S. Supreme Court concerning public employees in which the Court rejected the argument that "public employees can never have a reasonable expectation of privacy in their place of work." O'Connor vs. Ortega, 480 U.S. 709, at 717 (1987). In *O'Connor* the Court examined the issue as to what extent a public employee has a right to privacy. Opining that the employer must address this on a case-by-case basis, regardless of whether the employee works in the public or private sector, the court stated that "public employees' expectation of privacy in their offices, desks, and file cabinets, like similar expectation of employees in the private sector, may be reduced by virtue of actual office practices and procedures, or by legitimate regulation." *Id.*

Employers may also transfer data to third countries not providing adequate protection if such a transfer is "necessary." One of the scenarios most frequently raised is an employer wishing to transfer business-related information regarding its employees internally within the company. For example, a company may want to share the contact information of each employee with all other employees via a centralized database in the United States. Unless the employees consent unambiguously, a company may not even transfer information such as this, which common sense would lead most people to conclude is not data that is in need of protection, under article 26(1) of the Directive since, within the meaning of article 26(1), the company does not need to transfer the data for the performance of the employment relationships.[152] The same applies to the transfer of information including the administration of payroll and stock options. Since it is generally not "necessary" for a company to transfer such data outside the EU, the prevailing view is that a company may not transfer such data to a country not providing adequate protection solely on the basis of article 26(1).

The EU meant the derogations of article 26(1) to be limited in scope, and companies should not rely on them to justify the transfer of protected personal information from the EU. In fact, the article 29 Working Party has taken the position that "it is preferable to rely on adequate protection in the country of destination rather than relying on the derogations listed in article 26" to comply with the Directive's principles.[153] Further, a number of EU countries, Italy for example, have construed article 26(1) very narrowly in their national laws.[154] Employers should be aware that they run the risk of facing sanctions if they erroneously apply article 26(1).

B. The Risks of Noncompliance

It is a well-known secret that, even though member states have the authority to impose sanctions on companies breaching data privacy laws, the enforcement of these laws has been relatively lax to date. Spain is the most notable exception as its data protection authorities have pursued an extensive number of cases.[155]

152. Scheer, *supra* note 14 (discussing General Motors' troubles when it sought to set up an electronic phone book of its employees which involved transferring data regarding its EU employees outside the EU). General Motors ended up concluding contracts, either standard contractual clauses or ad hoc contracts, to transfer the data. General Motors is also self-certified under the Safe Harbor.

153. Working Party Opinion 8/2001, *supra* note 19, at 26.

154. EU Committee of the American Chamber of Commerce in Belgium Position Paper on the Review of Directive 95/46/EC on the Protection of Individuals with regard to the Processing of Personal Data, Aug. 7, 2002, at 6, *available at* http://www.eucommittee.bc/Pops/2002archive/dataprotection82002.pdf.

155. Of the EU countries, the Spanish data protection authorities seem to be the most active. The Spanish data protection agency has grown significantly since the harmonization of the Directive into Spanish national law. For example, in 2002, this agency initiated 723 investigations. *See* Agencia Española de Protección de Datos, at https://www.agpd.es/index.php (last visited Mar. 5, 2005). Fortunately, the agency is quite efficient as of the over 700 investigations that were initiated in 2002, nearly 441 were concluded within the same year. *Id.* Parties wishing to appeal the decisions of the Spanish agency should proceed with caution since, of the 153 appeals in 2002, only nine were successful or partially successful. *Id.* The rest were denied. *Id.* Two cases that garnered a significant amount of attention were the fines of Microsoft in Spain for violating Spain's data privacy laws (Microsoft paid a fine of approximately $60,000) in preparation for its Windows 98 rollout and of Spain's telephone company, Telefonica, for approximately $160,000 for violating Spain's data privacy laws. *Id.*

Under the Directive, both employees[156] and the data protection authorities[157] have a right of action for the violation of a country's data privacy laws. The level of liability depends on the laws of the respective country. Not surprisingly, sanctions vary from jurisdiction to jurisdiction, ranging from civil fines, imprisonment, seizure of files or data, to injunctive relief that could block the transfer or require a cessation of data processing activities. The penalties that data protection authorities may impose depend on the jurisdiction. In Spain, if a party commits a "very serious infringement" it may be subject to a fine of up to approximately 600,000€.[158] In Germany, the maximum fine is 250,000€[159] or a prison sentence of up to two years,[160] while in Austria it is up to 19,000€[161] so long as it is only an administrative offense instead of a criminal offense, which is greater in magnitude than an administrative offense. In Ireland, the fine is up to 100,000€.[162] A violation of Greece's data privacy laws could lead to a fine in excess of 140,000€.[163]

It should go without saying that businesses processing and transferring data from the EU to countries lacking adequate protection need to keep themselves abreast of the potential risks involved in engaging in such transactions illegally.

IV. Regulations for Employee Data Protection

One question that the European Commission has recently raised is whether it is necessary to have legislation that specifically addresses processing and transferring personal data in the employment context. As this article has already discussed, it is clear that the Directive applies to human resource matters; however, so far this article has applied only general data privacy principles to the employment arena and has *not* discussed a directive that applies specifically to employment relationships.

Some commentators question whether the Directive and the Directive on Privacy and Electronic Communications[164] are sufficient to protect employees and their right to privacy.[165] As such, a number of member states adopted rules or recommendations specifically

156. Directive, *supra* note 4, art. 22, at 45 (stating "... member states shall provide for the right of every person to a judicial remedy for any breach of the rights guaranteed him by the national law applicable to the processing in question.").

157. *Id.* art. 28(3), at 47 (stating, "Each authority shall in particular be endowed with: ... the power to engage in legal proceedings where the national provisions adopted pursuant to this Directive have been violated or to bring these violations to the attention of the judicial authorities."

158. Spain Organic Law 15/1999, *supra* note 22.

159. German Federal Data Protection Act, *supra* note 17, § 43(3).

160. *Id.* § 44(1).

161. § 52(1) Data Protection Act 2000 (*Datenschutzgesetz 2000*) BGBl 165/1999 [hereinafter Austrian Federal Data Protection Act].

162. Data Protection Act 1988, §31, as amended (2003).

163. Article 21 Law 2472/1997 on the Protection of Individuals with Regard to the Processing of Personal Data, as amended, *available at* http://www.dpa.gr/Documents/Eng/2472engl_all.doc.

164. Council Directive 2002/58/EC, 2002 O.J. (L 201).

165. *See* Commission Second Stage Consultation of Social Partners on the Protection of Workers' Personal Data, Annex, at http://europa.eu.int/comm/employment_social/news/2002/oct/data_prot_en.pdf [hereinafter Second Stage Consultation] (setting forth the views of several organizations concerning a proposed directive concerning personal data in an employment context); Ulrike Fleck, *Brauchen wir ein Arbeitnehmerdatenschutzgesetz!*, BETRIEBS-BERATER, Feb. 5, 2003, at 306 (debating the necessity of introducing legislation in Germany concerning data privacy in an employment context); Marcel Grobys *Wir brauchen ein Arbeitnehmerdatenschutzgesetz*, BETRIEBS-BERATER, Mar. 26, 2003, at 682 (also debating the necessity of introducing legislation in Germany concerning data privacy in an employment context).

concerning the processing of employees' personal data in some form.[166] The rules are, of course, not uniform, which leads the Commission to conclude that data protection rules in the employment arena are too fragmented, causing unpredictability and inefficiencies.[167]

Beginning in August 2001, the Commission undertook a formal consultation process to examine the necessity of an additional directive, concluding that such a directive may very well be necessary and would indeed add value. It was initially anticipated that the Commission would decide whether such a directive is necessary sometime during the course of 2004 or 2005.[168] It has since become clear that this will have to wait until sometime after 2005.

Although such a directive is still only in the preliminary phase, its focus is already clear. It would concentrate on the following issues: (1) employee's consent for the processing and transferring of personal data; (2) monitoring and surveillance at the work place; (3) processing health and medical data; and (4) processing drug testing and genetic testing data.

As discussed above, processing and transferring personal data based only on an employee's consent is already a thorny issue. Indeed the Commission states in its Second State Consultation, "[t]he role consent can play in an employment relationship, as a means [of] legitimizing the processing of workers' personal data, including their transfer to third countries, is quite controversial, because of the dependent and subordinate situation of the worker."[169] The proposed directive will set forth the principles employers must adhere to when processing and transferring data based on an employee's consent.

While it does not seem very likely at this time, it remains to be seen whether a new directive will indeed add any value or whether it will only add complexity to an already complex issue. There is real risk that a new directive would add more regulation to an area of law that is already confusing, and as a result, employers would be even less prone to observe the terms of a new directive.

The second aspect of the proposed directive concerns an employer's right to monitor and engage in surveillance of employees at the work place, even though the current Directive already applies to such activities.[170] The surveillance and monitoring relates not only to the use of the telephone, email, the Internet, and other means of electronic communication, but also to the use of cameras and videos at the work place. The Commission recognizes that technology has developed to such a great extent that employers have any number of alternatives available to monitor their employees. The Commission's concern is that employers may abuse this power, crossing the line from engaging in surveillance for legitimate business-related reasons to invading an employee's privacy. This concern becomes increasingly relevant as fewer and fewer employees are working in the traditional work-place setting while more are working from home, have been outsourced, or are work-

166. Finland has adopted legislation; Sweden and Belgium have proposed legislation; and France, Greece, the Netherlands, and the United Kingdom have issued opinions, recommendations, or codes of conduct. Second Stage Consultation, *supra* note 165, at 6.

167. *Id.* at 8.

168. Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions: Mid-Term Review of the Social Policy Agenda, June 2, 2003 (COM(2003) 312 final), at 16, *available at* http://europa.eu.int/comm/employment_social/social_policy_agenda/COMM_PDF_COM_2003_0312_F_EN_ACTE.pdf.

169. Second Stage Consultation, *supra* note 165, at 11.

170. Directive, *supra* note 4, Recital 14, at 32 (stating the Directive applies to data that is "used to capture, transmit, manipulate, record, store or communicate sound and image data relating to natural persons.").

ing in other non-traditional settings. In short, the line between working time and personal time is constantly becoming more blurred.

The most likely outcome is that the new proposed directive would require employers to consult with employees, or, if applicable, employee representatives, before monitoring or engaging in the surveillance of employees. Even then, employers would only be permitted to track or monitor employees for health, safety, or security reasons, or if there is a reasonable suspicion of a crime. Employers would not be permitted to conduct random checks of an employee's emails or telephone calls without having recognized grounds for doing so, thereby placing the onus on employers to demonstrate that they are not invading the employees' privacy. Although these provisions are in line with existing law, proponents argue that their codification may be necessary, or at least advisable, since many of these points have been developed only through case law or data privacy treatises. Codification into the national laws of each of the EU member states would give these provisions greater credence and provide greater predictability.

The last two aspects of the proposed directive, processing health and medical data and engaging in drug testing and genetic testing data, are attributable largely to the technological advancements made in these fields. For example, it has become increasingly simple for employers to conduct drug testing at the work place. The new directive would set forth that consent alone should not be used as a basis for engaging in drug testing; instead, employers should be permitted to use this form of testing only for legitimate reasons, including, most notably, to ensure that an employee or a potential employee is fit for a particular position. Further, only qualified medical personnel should conduct such testing, and the information derived therefrom must remain confidential. Similarly, employers should use genetic testing only in very exceptional cases for health and safety reasons. Along the same lines as monitoring and surveillance, employers must ensure that they do not cross the line of invasion of privacy by engaging in drug or genetic testing.

V. Conclusion

Data privacy remains a constant source of discussion among companies and their advisors. Unfortunately, because it is still a relatively new topic, many companies find themselves unprepared. Further, because enforcement has been lax, companies have not given as much attention to this topic as may be warranted. Still, one thing is certain: data privacy, data privacy laws, and data privacy authorities are here to stay. In fact, some say that today's data privacy laws are comparable to yesterday's product liability laws, which were not given great attention by employers during the initial phase of the industrial revolution. Their enforcement was haphazard at best. However, they eventually became a significant part of the commercial and industrial world. Data privacy laws may very well some day garner the same attention that product liability laws currently enjoy.

Hopefully, this article clears up some of the misconceptions regarding data privacy, at least in the employment arena, and gives companies some direction when deciding what data privacy avenue is most suitable to follow.