INTERNATIONAL HR JOURNAL
WINTER 2009 VOL. 18, NO. 1

THE IMPACT OF EU DATA PROTECTION LAWS ON U.S. GOVERNMENT ENFORCEMENT INVESTIGATIONS

Breon S. Peace and Jennifer A. Kennedy

Recent years have seen a sharp rise in the number of complex regulatory and criminal investigations, such as insider trading and Foreign Corrupt Practices Act cases, involving companies that are based abroad or have relevant information located abroad.[1] One consequence of this trend is the increased (and sometimes unforeseen) effect of the European Union's data protection requirements on corporations responding to requests for information or documents located overseas.

The EU and its Member States have created a far-reaching framework regarding the protection of personal information that applies to the collection, processing, and/or transfer of such information (electronic or otherwise). Therefore, a party that requires data located in the EU during an investigation by the United States Department of Justice, the United States Securities and Exchange Commission, or other U.S. authority needs to consider the legal implications of the EU framework on the protection of personal information.

BREON S. PEACE is a Partner and JENNIFER A. KENNEDY is an Associate at Cleary Gottlieb Steen & Hamilton LLP.

I. THE EU DATA PROTECTION DIRECTIVE

In 1995, the Parliament and Council of the European Union adopted Directive 95/46/EC on the protection of individuals with regard to the processing of personal data concerning individuals and the free movement of such data (the Directive).[2] The Directive applies to data protection not only in the twenty-seven Member States of the EU,[3] but in the European Economic Area countries as well.[4] The Directive aims to protect the fundamental rights and freedoms of natural persons, and in particular, their right to privacy of personal data as guaranteed under the European Convention on Human Rights and the Charter of Fundamental Rights of the European Union. Each Member State has adopted implementing legislation consistent with the Directive.

The Directive generally prohibits the personal data of natural persons from being processed or transferred unless specific conditions are met.[5] Under the Directive, personal data is broadly defined to include any information relating to an identified or identifiable natural person, including any factor specific to the person's physical, physiological, mental, economic, cultural, or social identity contained anywhere, including documents, electronic material, sound recordings, and image recordings.[6] "Personal data" includes a person's name, address, national identity number, birthday, religious or political affiliation, place of employment, job title, credit card number, medical records, photographs, voice recordings, and criminal records.[7] Information remains personal data even if it is available from a public source, such as the Internet. The Directive applies only to "natural persons," but some EU Member States have expanded the definition of natural persons to include deceased persons and certain busi-

ness entities.[8] Under the Directive, "processing" is defined as any operation or set of operations performed by electronic means on personal data, including, but not limited to, collecting, recording, organizing, storing, retrieving, transmitting, erasing, or destroying.[9] This would include, for example, the retrieval of e-mails containing the names and job titles of their senders and recipients—a commonplace task necessary to respond to government requests for information.

Accordingly, the collection and transfer of personal data from an EU Member State to the United States for purposes of compliance with a U.S. government agency request are governed by the Directive and the data protection laws of the EU Member States where such data is located. Separate provisions of the Directive apply to processing that is done wholly within an EU Member State and transferring personal data outside of an EU Member State, although there is significant overlap among the provisions.[10]

II. TRANSFER AND PROCESSING OF PERSONAL DATA

The Directive provides that personal data may be processed within an EU Member State under six circumstances: (1) with the consent of the data subject; and without consent (2) if it is necessary for the performance of a task carried out in the public interest or in the exercise of official authority;[11] (3) if it is necessary for compliance with a legal obligation (*e.g.*, a subpoena from a Member State or to comply with the administrative law of a Member State);[12] (4) if processing serves the legitimate interests pursued by the party to whom the data will be disclosed, except where such interests are overridden by the fundamental rights and freedoms of the data subject;[13] (5) when it serves the vital interest of the data subject; and (6) when necessary under a contract.[14]

The Directive separately addresses the circumstances under which personal data may be transferred outside of an EU Member State.[15] In determining whether such a transfer is permissible, the Directive distinguishes between countries that provide an adequate level of protection for data, meaning a level of protection similar to the Directive, and those that do not.[16] The circumstances under which personal data may be transferred into a country that does not have an adequate level of protection are narrower than those governing transfer of personal data into a country with adequate protection. The EU has found that the United States does not offer an adequate level of protection.[17]

Transfer of personal data to the United States, or any other country without an adequate level of protection, may be made only under circumstances that justify processing of personal data (1) with consent, (2) when it serves the vital interest of the data subject, and (3) contractual necessity.[18] In addition, transfer may occur if it is necessary or legally required on important public interest grounds, or for the establishment, exercise or defense of legal claims.[19]

Under the Directive, personal data may be transferred from an EU Member State if the data subject (*i.e.*, the natural person whom the data concerns) unambiguously consents to the transfer.[20] Consent must be freely given and the data subject must be given the details regarding the content of the data to be transferred, the purpose of the transfer, and the length of time the data will be available for the defined purpose. While all Member States allow consent as a basis for the transfer of personal data, some consider an employer's request for consent from an employee to be inherently coercive.[21] Therefore, when seeking an employee's consent, employers must take special care to develop and document a process that demonstrates that the employee's consent was obtained in a non-coercive manner.[22]

The Directive's allowances for transfer (other than by consent) are generally viewed as exceptions to the consent requirement and therefore are usually interpreted narrowly. For example, the exception for data vital to the subject refers to medical necessity or the like. The exception for contractual necessity, however, includes a contract that implies that certain personal data will be transferred (*e.g.*, travel agent disclosing personal information to a hotel).

While the exception based on public interest considers only the interests of EU Member States, parties seeking transfer to the United States to comply with requests of a U.S. authority have argued to the relevant national data privacy authority that the interests of such authority and the EU are aligned (*e.g.*, ensuring the stability of international financial markets or safe import/export of goods). Such arguments have had some success under tax and customs law, as the Directive specifically mentions compliance with customs and tax laws as matters

that would be in the interest of the EU.[23]

As for the allowance of transfer from the EU if it is necessary for the establishment, exercise, or defense of legal claims, that too is interpreted strictly. Compliance with a voluntary request for information or transfer of information that is not clearly necessary to defend against a legal claim is unlikely to be permissible, nor is transferring personal data for purposes of an internal investigation that is related only to potential legal claims or defenses. Member States may differ as to whether a subpoena from a U.S. authority is sufficient to allow transfer under the "necessary for defense of a legal claim" exception, but the EU has consistently held that only the laws and obligations of a party as defined by each Member State and the EU are appropriately considered when determining the permissibility of personal data transfers. For example, the Article 28 Working Party, in considering whether export by SWIFT of data concerning international money transfers to the United States and its subsequent disclosure under subpoena of such data to U.S. anti-terror authorities was permissible, found that the subpoena was not covered by the "legally required/needed for defense of legal claims exception because the transfer was not necessary or legally required under the law of an EU Member State."[24] According to the Working Party, "any other interpretation would make it easy for a foreign authority to circumvent the requirement for adequate protection in the recipient country."[25] Thus, a subpoena from a U.S. authority may not be sufficient to allow for transfer of personal data to the United States from the EU.

In all the circumstances under which transfer is allowed, the data subject is entitled to notice, unless such notice would compromise the purpose of the transfer (*e.g.*, a criminal investigation).[26] Further, if transfer is permissible it must be done fairly and with the utmost respect for the privacy of the data subject.[27] More specifically, the personal data may only be transferred for the specified, explicit, and legitimate purposes and not further transferred in a way incompatible with those purposes.[28] The personal data transferred must be adequate, relevant, and not excessive in relation to the purposes for which it is processed and transferred.[29] The personal data transferred must be accurate and up to date.[30] And, personal data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the data was collected and transferred.[31]

III. SANCTIONS FOR VIOLATIONS OF DATA PROTECTION LAWS

Under the Directive, each Member State is required to establish a national data authority to adjudicate matters relating to the implementation of data protection laws and to provide guidance to entities wishing to process or transfer personal data.[32] Member States are also required to adopt sanctions for violations of their data protection laws, with a judicial remedy (including potential compensation) for any breach.[33] Generally, Member States provide for administrative fines and, in rare cases, criminal sanctions (of up to three years imprisonment) for non-compliance with data protection laws.[34] Germany has the highest allowable administrative fine for violations of its data protection laws, euro 250,000 (at the current exchange rate, U.S. $380,000) per violation.[35] In all Member States, a data subject can bring a civil suit for damages for violations of his or her rights under the Member State's data protection law.[36]

In April 2007, French authorities imposed a euro 30,000 fine on Tyco Healthcare France, a subsidiary of Tyco Healthcare, a company based in the United States (collectively, Tyco). The fine related to Tyco's transfer of information regarding its European employees to the United States for purposes of managing salaries on a global scale. The information transferred included names, identification numbers, addresses, job titles, and salaries. Under France's data protection laws, Tyco was required to seek authorization from the French data protection authority for the transfer of such personal information of any French citizen outside of France. While Tyco did seek this permission, it did so only retroactively, after the transfer of the information began, and it continued to transfer the information while the request was pending. The French authority found the retroactive request a violation of the data protection laws. The French authority criticized Tyco's conduct during its inquiry, finding, after several requests, that Tyco had not been forthcoming with the French authorities and that the transfers had remained ongoing in spite of Tyco's representation that it would cease the transfers. While the fine appears to be the

first levied against a U.S.-based multi-national corporation for violation of data protection laws of a Member State of the EU, it demonstrates the importance EU Member States place upon compliance—with data protection laws and the privacy of—EU citizens.

IV. COMPLYING WITH THE DIRECTIVE

Clearly, then, when an entity must respond to a U.S. authority requesting information that is located in the EU, the Directive must be considered. The first step in assessing how to proceed is to determine which Member State's national data protection law applies. The general rule is that the location of the entity that will do the processing or transferring governs, but, as with choice of law determinations in the United States, this assessment can be complicated and challenging, and so consultation with experts in the field of EU data protection and counsel learned in the data protection laws of the relevant Member State may be required.

Next, the entity will have to determine whether the data may be processed at all under the circumstances. As noted above, the entity may seek consent to process the data or may process under certain narrow circumstances. If the entity is permitted to process the data, the difficult issue arises whether a transfer to the U.S. authority is permissible. As discussed above, there are a few circumstances under which transfer is allowed, but the Directive and Member States' data protection laws can pose a significant obstacle to a corporation's ability to directly provide U.S. authorities with information. Absent valid consent or a clear legal obligation to process or transfer the data, the entity may not be permitted to provide personal data to U.S. authorities. This is particularly problematic with respect to voluntary requests for information: absent valid consent by the subject, compliance with a voluntary request would seem especially difficult to justify under the Directive in most cases.

If the transfer is not permissible under the law, the entity could consider alternatives to attempt to satisfy the U.S. authority. First, it may request that the relevant national data authority give specific permission for the transfer of the information. In support of the request, the entity could argue that it is in the Member State's interest to allow the transfer and such interest outweighs the privacy rights at stake. Such a request may take several months to be reviewed. Also, the entity may consider transferring the requested information in redacted form, removing all personal data that is protected from disclosure. Not only can this process be extremely time consuming and costly, but redacted materials may not satisfy the U.S. authority.

Because responding to a request from a U.S. authority seeking information in the EU is complicated and time-consuming, it is important to keep the U.S. regulator informed about efforts to comply with the request. Of course, depending on which EU Member State is implicated, the nature of the investigation, and the needs of the U.S. authority, the ultimate answer may be that the corporation is not permitted to transfer data to the United States. U.S. regulatory and criminal authorities are becoming increasingly aware of the obstacles the Directive presents. At the same time, however, many entities have been transferring personal data to U.S. authorities without full consideration of the Directive, and, accordingly, a U.S. authority may be reluctant to accept unsupported claims that the Directive prevents transfer. Entities concerned about violating the Directive or Member States' laws for transferring information to a U.S. authority should therefore be prepared to provide support, typically in the form of an opinion from counsel, for a claim that such transfer would be unlawful.

While the inability to obtain documents from an entity will prove frustrating to a U.S. authority, it is not the end of the line for its investigation. U.S. regulatory and criminal authorities may have other avenues for obtaining information located in the EU. For example, in 2002, the SEC entered into a Multilateral Memorandum of Understanding with the International Organization of Securities Commissions.[37] Thirty-four securities and derivatives regulators are currently signatories of the MMOU, which, among other things, provides that the signatories will share information and documents held in the regulators' files.[38] In addition, the SEC has signed bilateral information-sharing Memoranda of Understanding with the securities authorities of twenty countries, including EU Member States such as France, Germany, Italy, the Netherlands, and the United Kingdom.[39] The bilateral MOUs are generally similar to the MMOU in that they allow for the sharing of informa-

tion between securities authorities, with provisions relating to the uses and confidentiality of any information shared. Through the MMOU and the various MOUs, the SEC may obtain information directly from the EU securities regulators.[40] Even if an EU Member State is not a party to the MMOU or a bilateral MOU, its securities regulators may still cooperate with the SEC on an *ad hoc* basis to find alternative ways to obtain the information needed.

Similarly, the DOJ has entered into Mutual Legal Assistance in Criminal Matters Treaties, or MLATs, with a number of EU Member States. The MLATs permit direct communication between the justice departments of these Member States and the DOJ with respect to criminal matters and include agreements to invoke national law to compel the production of documents in the one nation to assist another nation's criminal authority.[41]

V. COLLATERAL EFFECTS

Entities considering how to respond to a U.S. authority's request for information that is covered by the Directive need to carefully consider the collateral effects of its response. For example, the SEC, the DOJ, and many other U.S. authorities, take into account a corporation's level of cooperation when assessing whether to pursue an action against the corporation and how to resolve any such action. If the U.S. authority has the ability to get the information it has requested in some way that clearly would not violate the Directive, such as through an MOU or MLAT, the corporation should consider what, if any, benefit there is in forcing the U.S. authority to pursue this alternative. For highly-regulated entities, the long-term effects on the relationship between the entity and the U.S. regulator should also be considered. Further, the effects of the response on the investigation immediately at hand, including whether declining to respond to a voluntary request for information will lead to escalation of the investigation, are important factors in determining when and how to respond to the U.S. authority regarding the application of the Directive. And, corporations must take into account the risk that information disclosed to U.S. authorities will be discoverable by third parties in the United States.[42]

If a direct transfer is nevertheless to be made to a U.S. authority pursuant to consent or a recognized exception, discussions regarding the notification and specific purpose requirements of the Directive should be had by the employer with the relevant employees. When asked for consent or notified of a transfer, the employees should generally be informed that their information is being transferred and for what purpose, and that the U.S. authority may transfer the data onward to other U.S. authorities for purposes of enforcing U.S. laws. The employer should inform the U.S. authority of the nature and content of such employee notification. The employer should also discuss the scope of the request with the U.S. authority, as the Directive requires that only information that is absolutely necessary for the specific purpose be processed and transferred. As most requests from U.S. authorities are very broad in scope, this is an essential discussion.

VI. CONCLUSION

While the European Commission has undertaken efforts to make compliance with the Directive manageable in a global economy,[43] these efforts do not address the dilemma of global corporations faced with requests for information in connection with regulatory or criminal investigations in the United States. Experience and expertise in responding to such requests is key both for complying with the Directive and for satisfying obligations to U.S. authorities. As Tyco discovered, matters of personal privacy are taken seriously in the EU and the notion that what an employee does, writes, or says at work is the employer's business is rejected by the EU, which holds that an individual's personal privacy is not abandoned in the workplace. ■

NOTES

1. *See* Sheri Qualters, "Risk of Bribe Probes Grows for Business," 1/7/2008 *Nat'l L.J.* 08 ("The DOJ brought 16 FCPA enforcement actions in 2007, compared with just three in 2004. The FBI has seventy-seven pending FCPA investigations."); *see, e.g.*, Complaint, *SEC v. Sonja Anticevic,* No. 05 Civ. 6991 (KMW), 2005 WL 2583142 (S.D.N.Y. Aug. 5, 2005) (alleged international insider trading ring); Complaint, *SEC v. Jim Bob Brown,* H 06-2919, 2006 WL 3099446 (S.D. Tex. Sept. 14, 2006) (alleged three schemes to bribe foreign officials).
2. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *Official Journal of the European Communities of 23 November, 1995,* No L. 281 (available at http:// www.cdt.org/privacy/eudirective/EU_Directive_ .html).
3. The EU Member States are Austria, Belgium, Bulgaria, the Czech Republic, Cyprus, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Italy, Ireland, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Poland, Portugal, Romania, Spain, Slovakia, Slovenia, Sweden, and the United Kingdom.
4. The countries that are in the EEA but not

in the EU are Iceland, Lichtenstein, and Norway. Switzerland is not a member of the EEA and Swiss nationals are not EU citizens, but, under a bilateral agreement between the country and the EU, Swiss nationals have similar rights as EU citizens.

5. The Directive does not apply to processing operations relating to public security, defense or Member State security and criminal law. It stipulates that processing of data relating to offenses, criminal convictions, or security measures be carried out under the authority of each Member State. In 2006, the European Court of Justice annulled an agreement between the European Community (EC) and the United States on the transfer of passenger name records from EU air carriers to the United States on the basis that the EC was acting in the area of public security, in which it has no competence. *See* Mario Mendez, Passenger Name Record Agreement European Court of Justice: Annulment of Commission Adequacy Decision and Council Decision Concerning Conclusion of Passenger Name Record Agreement with US Grand Chamber Judgment of 30 May 2006, Joined Cases C-317/04 and C-318/04, *European Parliament v. Council and Commission,* 3 *European Const. L. Rev.* 127 (2007).
6. Directive, Art. 2(a).
7. The Directive applies more stringent requirements to the processing of "sensitive data" including racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, health, and sex life. Directive, Art. 8.
8. Denmark has extended protection to deceased persons. Austria, Italy and Luxembourg have extended protection to legal persons, entities, and associations.
9. Directive, Art. 2(b). Some EU Member States, such as Germany, have expanded the definition of processing to tasks carried out manually.
10. Directive, Ch. II, IV. Chapter II deals with processing of personal data, while Chapter IV deals with the transfer of personal data.
11. The terms "public interest" and "official authority" as used in the Directive both refer to that of EU Member States. Thus, the interest of the United States or a United States' agency would not satisfy this necessity test.
12. Directive, Art. 7(a). Again, the laws of the EU or its Member States, not the laws of the United States, are relevant for the purposes of determining whether a legal obligation exists.
13. This is essentially a balancing test. Most Member States assign a heavy weight to the privacy rights of the data subject, and, accordingly, the legitimate interest must be of great importance to overcome these rights. For example, surveillance of all employees at a bank to deter bank robberies likely meets the legitimate interest test.
14. Directive, Art. 7. However, the Directive specifically provides that each Member State may determine more precisely the circumstances under which processing may occur. Indeed, most EU Member States have introduced variations from the basic provisions contained in the Directive. Thus, the specific provisions of a Member State's data protection law must be consulted.
15. Directive, Ch. IV.
16. Directive, Art. 25.
17. A country is considered to provide an adequate level of protection for personal data if it guarantees standards equivalent to those provided within the EU. The Freedom of Information Act is routinely cited as a reason why the United States does not offer an adequate level of protection for personal data. *See* Opinion 1/99 of the Article 29 Data Protection Working Party (adopted January 26, 1999).
18. Directive, Art. 26(1). Again, the Directive specifically provides that each Member State may define these circumstances differently.
19. Directive, Art. 26(1).
20. Directive, Art. 7(a).
21. The Article 29 Data Protection Working Group has stated: "The Article 29 Working Party takes the view that where as a necessary and unavoidable consequence of the employment relationship an employer has to process personal data it is misleading if it seeks to legitimize this processing through consent. Reliance on consent should be confined to cases where the worker has a genuine free choice and is subsequently able to withdraw the consent without detriment." *See* Opinion 8/2001 of the Article 29 Data Protection Working Party at 23 (adopted Sept. 13, 2001). Also, under the Belgian Data Protection Act, for example, consent for processing "sensitive" personal data may not be obtained in the employer-employee context. *See L'arrté royal portent exécution de la loi du 8 décembre 1992 relative à la protection de la vie privée a l'égard des traitements de données à cractére personnel, Art. 27 (2001).*
22. One method that may qualify as non-coercive is acquiring consent in advance of any specific need to process or transfer through the adoption of company-wide standards of conduct, which employees must read and acknowledge, alerting employees to the possibility that their personal data may be processed or transferred for certain defined purposes, including responding to a U.S. government request. However, an employer should consult with local counsel to determine if such standards of conduct would be sufficient in the relevant Member State. To achieve greater certainty, such standards of conduct can be sent to the relevant Member States' data authority for approval prior to adoption.
23. See Directive, Art. 58.
24. Opinion 128 of the Article 28 Data Protection Working Party, ¶ 4.6.3.4.
25. Opinion 128 of the Article 28 Data Protection Working Party, ¶ 4.6.3.4.
26. Directive, Arts. 10, 11.
27. Directive, Art. 6(1)(a).
28. Directive, Art. 6(1)(b).
29. Directive, Art. 6(1)(c).
30. Directive, Art. 6(1)(d).
31. Directive, Art. 6(1)(e).
32. Directive, Art. 28.
33. Directive, Arts. 22, 23.
34. See, e.g., L'arrté royal portent exécution de la loi du 8 décembre 1992 relative à la protection de la vie privée a l'égard des traitements de données à cractére personnel, art. 41 (2001); Loi relative à l'Informatique, aux Fichiers et aux Libertés, arts. 47, 50-52 (2004); Codice in Materia di Protezione dei Data Persoanli, art. 161-172 (2004).
35. *See* Federal Data Protection Act (*Bundesdatenschutzgesetz*), §§ 43, 44.1 (2001).
36. Directive, Art. 22.
37. *See* http://www.sec.gov/about/offices/oia/oia_crossborder.htm.
38. *See* http://www.sec.gov/about/offices/oia/oia_crossborder.htm.
39. *See* http://www.sec.gov/about/offices/oia/oia_crossborder.htm.
40. The SEC and the German Federal Financial Supervisory Authority signed an MOU in April 2007. In announcing the MOU, SEC Chairman Christopher Cox highlighted the usefulness of the MOU allowing "access to the information necessary to supervise global securities firms and oversee markets." SEC, "German BaFin Sign Regulatory Cooperation Agreement, Apr. 26, 2007" (available at http://www.sec.gov/news/press/2007/2007-76.htm).
41. *See* Thomas G. Snow, "The Investigation and Prosecution of White Collar Crime: International Challenges and the Legal Tools Available to Address Them," 11 *Wm. & Mary Bill Rts. J.* 209 (2002).
42. *See Ratliff v. Davis Polk & Wardwell,* 354 F.3d 165 (2d Cir. 2003) (holding documents from an accounting firm in the Netherlands possessed by U.S. law firm that were voluntarily provided to SEC were subject to discovery from the law firm).
43. In an attempt to facilitate international commerce while maintaining the privacy rights of EU citizens, the European Commission has authorized the transfer of personal data among business entities within and outside the EU if such entities adopt contractual clauses mirroring the provisions of the Directive. Furthermore, as to the United States, the EU has entered into a Safe Harbor Agreement, which allows U.S. companies that adopt the safe harbor requirements, which are similar to the provisions of the Directive, to receive personal data from the EU. *See* http://www.export.gov/safeharbor.