

# **Conflict of Interests: EU Data Protection Statutes and US Corporate Investigations**

By David F. Axelrod  
Forensic & Dispute Services  
Deloitte Financial Advisory Services LLP

*This article originally appeared in the August, 2008 edition of The Champion, a publication of the National Association of Criminal Defense Lawyers.*

# **Conflict of Interests: EU Data Protection Statutes and US Corporate Investigations**

**By David F. Axelrod  
Deloitte Financial Advisory Services LLP**

Throughout its history the United States has been regarded as a bastion of individual rights and a beacon for the Western world, making it ironic that citizens of the European Union (EU) today enjoy significantly greater protection than U.S. citizens of the sanctity of their personal data. Europeans' elevated sensitivity to this issue may be attributable to experiences with abuses of personal information by fascist and communist governments. Regardless, it can create enormous headaches for U.S. companies. While protecting their own citizens, EU data protection laws can become inimical to the interests of U.S. companies by, among other things, interfering with their ability to respond to demands for information by U.S. authorities, and to conduct cross-border investigations of suspected misconduct. In turn, this may prevent such companies from cooperating with the U.S. government in the manner contemplated by Department of Justice (DOJ) and Securities and Exchange Commission (SEC) policies.

The impetus for such investigations is well known. Sarbanes-Oxley and the mood surrounding it have created powerful incentives for corporations to go to great lengths and expense to uncover offenses and find culprits quickly. In typical corporate investigations, hard drives are imaged and employees interviewed. E-mail and correspondence are reviewed, and accounting data analyzed. Teams of outside counsel are engaged, assisted by outside consultants armed with laptops and note pads. Evidence is circulated far and wide by mail, facsimile and Internet. In investigations by the uninitiated, data protection rights are at most a secondary concern, and often an afterthought, if thought of at all. By ignoring or flouting data protection rights, companies sometimes create new problems while trying to manage old ones.<sup>1</sup>

It therefore is essential, when investigating on foreign soil, to become familiar with the local data protection landscape. This article, though far from comprehensive — this is an enormously complex subject — focuses on a few potential areas for collision between EU data protection laws and the interests of U.S. companies.

## **EU Directive 95/46/EC**

In response to European countries' differing approaches to data protection, in 1995 the European Parliament and the Council of Ministers adopted Directive 95/46/EC on the protection of individuals with regard to the processing of personal data<sup>2</sup> (the Directive), to establish uniform provisions governing the processing of personal data.<sup>3</sup> The Directive itself is not law. Rather, EU member states were required to enact their own implementing legislation and regulations to comply with the Directive, which became effective in 1998.<sup>4</sup> Eventually, all 25 EU member states managed to implement the Directive, including the 10 Central and Eastern European countries that most recently joined the EU.<sup>5</sup>

## **Restrictions on Processing Personal Data**

The Directive applies to public and private organizations, and those which, although not established in the EU, use equipment located there to process personal data.<sup>6</sup> It focuses primarily on the "processing" of "personal data,"<sup>7</sup> which is defined as any information relating to an identified or identifiable "data subject," or natural person.<sup>8</sup> "Processing" covers almost any operation involving personal data, including the collection, review, use and disclosure of personal data to any third party.<sup>9</sup> The

processing of personal data must be fair and lawful, for legitimate purposes, adequate, relevant, accurate and not excessive in relation to the purpose for which it was collected.<sup>10</sup>

For processing to be deemed fair, the data subject must ordinarily be notified of the recipient, the purpose for processing personal data and other information necessary to make the processing fair.<sup>11</sup> For it to be deemed legitimate, the data subject must consent, or the processing must be subject to one of several possible exceptions to the consent requirement. For present purposes, the most relevant may be that the processing is “necessary for compliance with a legal obligation to which the [data] controller is subject” or that processing is “necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed.”<sup>12</sup>

## **Restrictions on Transfer Outside the EU**

In addition to its restrictions on processing personal data, the Directive severely restricts the transfer of personal data to any non-EU country that does not afford the same privacy protections as EU member states<sup>13</sup> Article 26 contains certain “derogations” (exceptions) to this prohibition. For present purposes, the most relevant may be that “the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defense of legal claims.”<sup>14</sup>

Information about countries with inadequate protections is to be shared among Commission members.<sup>15</sup> The United States is specifically identified as not affording such protections because, rather than comprehensive government regulation, it relies on a combination of legislation, regulation and self-regulation.<sup>16</sup> The Department of Commerce, however, offers a voluntary “safe harbor” program, negotiated with the EU, through which participating companies may be deemed individually to provide adequate data protection.<sup>17</sup>

## **Sensitive Data**

Additional restrictions apply to, and the list of permissible purposes is shorter for, the processing of “sensitive” personal data, which includes “data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and the processing of data concerning health or sex life.”<sup>18</sup> Significantly, in some EU member states, information relating to offenses or criminal convictions may be deemed sensitive.<sup>19</sup> Thus, paradoxically, as knowledge of potential offenses increases, the ability to disclose them may decrease.

## **Impairment of Cross-Border Investigations**

These data protection rules can make life extremely difficult for lawyers who represent companies that do business on both sides of the Atlantic. This is especially true in their dealings with the DOJ and SEC, since in deciding whether to file criminal charges or bring a civil enforcement action, both emphasize whether a company has made a voluntary and complete disclosure.

## **The Value of Cooperation**

A non-exclusive list of the factors considered by DOJ attorneys in deciding whether to bring corporate charges is contained in the so-called “McNulty Memorandum,” a policy statement contained in Title 9 of the DOJ Criminal Resource Manual.<sup>20</sup> Similarly, some of the factors considered by the SEC in deciding whether to bring an enforcement action and what sanctions to seek are listed in the so-called “Seaboard Release.”<sup>21</sup>

Chief among the factors that the DOJ considers is “the corporation’s timely and voluntary disclosure of wrongdoing and its willingness to cooperate in the investigation of its agents.” This includes its “willingness to provide relevant evidence and to identify the culprits within the corporation.”<sup>22</sup>

The Seaboard Release differs from the McNulty Memorandum in that it was the SEC’s announcement of its decision in a particular case. In deciding not to act against a public company that had issued false financial reports, the SEC noted that the company “provided the [SEC] staff with all information relevant to the underlying violations ... [and] the details of its internal investigation, including notes and transcripts of interviews.” It then listed “some of the criteria [it] will consider in determining whether, and how much, to credit self-policing, self-reporting, remediation and cooperation,” including whether the company conducted a thorough internal investigation, and provided the Commission with a written investigative report and supporting documentation.<sup>23</sup>

There is obvious tension between the DOJ and SEC policies, on the one hand, and the Directive on the other, exacerbated by the narrowness of the exceptions to its restrictions. For example, an exception that is frequently considered in connection with transferring personal data to the United States as part of an investigation is that it is necessary “for the establishment, exercise or defense of legal claims.”<sup>24</sup> There may, however, be less to this exception than meets the eye, since in most EU member states, it may be required that the claims be imminent or at least expected. It is unclear whether this exception may be invoked where there is a mere likelihood of claims arising.<sup>25</sup>

Further limitations on this exception may compound the problem. Among other things, EU data protection authorities may regard a suspected violation of U.S. law alone as an insufficient basis to collect and transfer personal data to the United States, *i.e.*, a violation of the laws of an EU member state may also be required. Independently, they may regard the exception as inapplicable if the violations relate to a U.S. entity and not its EU affiliate. This may be especially troublesome where, for instance, an EU affiliate of a U.S. company is suspected of having paid bribes to foreign government officials in violation of the Foreign Corrupt Practices Act.<sup>26</sup>

Nevertheless, this miserly view of the legal claims exception is supported by a 2005 working paper of the Article 29 Working Party, an advisory body established under Article 29 of the Directive, with representatives from each EU member state. That working paper argues that the legal claims exception should be subject to “strict interpretation” and apply only where the legal claims relate to the EU Company transmitting the data rather than the foreign recipient. Furthermore, although Article 26(1)(d) also permits data transfers where “necessary or legally required on important public interest grounds,” the Working Party’s “strict interpretation” suggests that exception is unlikely to be available where the public interest arises solely in a non-EU state.<sup>27</sup>

### **Pervasiveness of Wrongdoing Within The Corporation**

In making its charging decisions, the DOJ also emphasizes “the pervasiveness of wrongdoing within the corporation, including the complicity in, or condonation of, the wrongdoing by corporate management,” *i.e.*, “the role of management.”<sup>28</sup> The SEC phrases it differently, but focuses on essentially the same considerations.<sup>29</sup> Obviously, to make this sort of determination may require a wide-ranging investigation, including a review of the personal data of many employees.

A review of such data in this situation may be irreconcilable with the Directive, even in the presence of a well-founded belief that one or more employees has engaged in criminal conduct. The application of potentially helpful exceptions may be “decidedly unclear” in such a wide-ranging investigation.<sup>30</sup> Furthermore, as noted above, under the laws of some EU member states, incriminating information may be deemed *ipso facto* sensitive. Thus, as more evidence is uncovered and

suspicious harden into actual knowledge, mere personal data may morph into sensitive data, triggering additional restrictions on its transfer. This, in turn, may interfere with a company's ability to disclose management's role in an offense. Nevertheless, this view is supported by another Article 29 Working Party paper that adopts a broad construction of the notion of sensitive data.<sup>31</sup>

## Other Headaches

There are many other aspects of the Directive and implementing statutes that have the potential to frustrate even the most well-founded and careful cross-border investigation. To cite two examples:

- Notice to the data subject is excused where necessary for “the prevention, investigation, detection and prosecution of criminal offenses.”<sup>32</sup> However, the Article 29 Working Party's view is that this requires a “substantial risk” of jeopardizing the investigation, and “must be applied restrictively, on a case by case basis.” Furthermore, EU member states do not all apply the exemption in a consistent fashion, and some do not apply it at all. And, even where the exemption may be invoked, there may come a point where providing notice will no longer jeopardize the investigation, and notice will have to be provided.<sup>33</sup>
- It is not uncommon for U.S. companies to have difficulty with EU data protection authorities when seeking to respond to disclosure demands by U.S. authorities that include data that resides with an EU affiliate. In such circumstances, the EU affiliate may have to apply to its local authorities for an order compelling the disclosure.<sup>34</sup>

## Skepticism by US Authorities

But, potentially the biggest headache may be skepticism by the U.S. authorities of an invocation of EU data protection statutes as a reason for not producing information. In some cases, U.S. law enforcement authorities may appreciate that a company may truly be caught between Scylla and Charybdis.<sup>35</sup> It may be penalized under EU law for producing information, or under U.S. law for withholding it. In such cases, it may be possible for the company and U.S. authorities to work together to find alternative solutions, such as the use of diplomatic channels, Mutual Legal Assistance Treaties and other means for a government-to-government transfer of information. Another possibility is to obtain a U.S. court order that may be enforceable in the EU under rules of international judicial assistance.

On the other hand, there may occasionally be good reason for such cynicism. “Strategically speaking, the data protection laws of the EU Member States ... offer various opportunities to avoid, limit or delay the discovery of unfavorable data stored in Europe.”<sup>36</sup> In other words, to use venerable Fifth Amendment parlance, EU data protection statutes may be used as “both a sword and a shield” against disclosure.<sup>37</sup>

There is historical precedent for the DOJ's challenging companies on this ground, albeit in a slightly different context. It did precisely that in 1984, in the highly publicized case of then-fugitive financier Marc Rich. On April 15, 1982, Marc Rich & Co. International (Rich & Co.), a wholly owned subsidiary of Rich's EU Company, was served with a grand jury subpoena *duces tecum* as part of an investigation of a suspected fraud involving crude oil price and allocation regulations.

Rich & Co. moved to quash the subpoena on grounds including that Swiss law prohibited the production of the materials demanded. The district court denied the motion, and eventually imposed on the company a fine of \$50,000 per day as sanction for civil contempt. Rich & Co. later moved to vacate the contempt sanction on the ground that directives of the Swiss government prevented it from complying with

the subpoena. After that motion was denied, Rich & Co. again moved to vacate, arguing this time that it was unable to comply because the Swiss government had seized certain of its documents.<sup>38</sup>

Although not reflected in the cited decision, the government argued (the author of this article was present in court) that the seizure was collusive, and in effect, that Swiss financial secrecy laws were being used as a sword and a shield to avoid disclosure. The rest is history: the contempt payments eventually totaled \$21 million; Rich's companies pleaded guilty to 78 felony counts and paid over \$150 million in fines; and, Rich remained a fugitive until being pardoned by President Clinton on January 20, 2001, his last day in office.

### **Treacherous Waters**

If this article has succeeded in clarifying only one thing, it should be that the transfer of personal data from the EU to the United States is both complex and fraught with peril. Sorting out the restrictions on processing and transfer, and their exceptions, can be daunting, even for local counsel in an EU member state whose statutes are at issue. But, for the successful conduct of a cross-border corporate investigation, this is as essential as it is difficult. These are, indeed, treacherous waters, which may be navigated safely only with a thorough understanding of local data protection laws.

## Notes

1. Daniel P. Cooper, Corporate Investigations & EU Data Protection Laws - What Every In-House Counsel Should Know (Covington Report 2006) (“What Every In- House Counsel Should Know”) at 1-2 (copies available at <http://www.cov.com/dcooper/>).
2. Official Journal of the European Communities; 1995 O.J.E.C.(L 281) 31-50.
3. See, e.g., Directive, Recitals 7-8.
4. Directive 95/46/EC, Art. 4 and 32. See George J. Terwilliger III, *Internal Investigations E.U. Data Protection Laws* (May 22, 2006 National Law Journal) (“Terwilliger”).
5. *What Every In-House Counsel Should Know*, at 4.
6. See Art. 2(d) and 3. *What Every In- House Counsel Should Know*, at 6.
7. Art. 3(1).
8. Art. 2(a).
9. See Art. 2(b).
10. Art. 6(1).
11. Directive, Recital 38.
12. Art. 7(c) and (f).
13. See Art. 25(1).
14. Art. 26(1)(d).
15. Art. 25(3).
16. See John Rosenthal and Stefan Hanloser, *European Union: European Data Protection Law v. E-Discovery Requirements Under US Law - How To Tackle the Dilemma* (April 8, 2008) (“Rosenthal and Hanloser”) (available at [www.mondaq.com/article.asp?articleid=59144](http://www.mondaq.com/article.asp?articleid=59144)).
17. 17.Terwilliger, at 2.
18. Art. 8(1).
19. *What Every In-House Counsel Should Know*, at 36.
20. [http://www.usdoj.gov/usao/eousa/foia\\_reading\\_room/usam/title9/crm00162.htm](http://www.usdoj.gov/usao/eousa/foia_reading_room/usam/title9/crm00162.htm).
21. SEC Release No.44969/October 23, 2001, available at [www.sec.gov/litigation/investreport/34-44969.htm](http://www.sec.gov/litigation/investreport/34-44969.htm).
22. *McNulty Memorandum*, at 4, 7.
23. *Seaboard Release*, at 3.
24. Directive, Art. 26(1)(d); *What Every In-House Counsel Should Know*, at 7-8.
25. *What Every In-House Counsel Should Know*, at 48.
26. 26.1d. at 49.
27. *What Every In-House Counsel Should Know*, at 53. There may be some movement in this area, however. The Working Party has included pretrial discovery on its 2008 agenda as a high priority. David J. Kessler and Peter A. Blenkinsop, *With ‘PreTria I Discovery’ an Official High Priority of the EU, Companies Need to Make EU Discovery and Data Protection a High Priority* (May 2008 The Metropolitan Corporate Counsel) (available at [www.metrocorpcounsel.com/pdf/2008/May/46.pdf](http://www.metrocorpcounsel.com/pdf/2008/May/46.pdf)). The authors of this article believe that the Working Party is likely to recognize the legitimate interest of multinational companies in complying with U.S. discovery obligations, though a particular company’s interests would still have to outweigh the interests of the data subject. *Id.* at 1-2.
28. *McNulty Memorandum*, at 4, 6.
29. *Seaboard Release*, at 3.
30. *What Every In-House Counsel Should Know*, at 32.

31. *What Every In-House Counsel Should Know*, at 36.
32. Art. 13(1)(d).
33. *What Every In-House Counsel Should Know*, at 46-47.
34. *What Every In-House Counsel Should Know*, at 49.
35. U.S. courts have occasionally been responsive to objections against discovery requests that would violate EU data protection statutes, Rosenthal and Hanloser, at 2, citing *Volkswagen v. Valdez*, 909 S.W.2d 900 (Tex. Sup. Ct. 1995). Such decisions, however, may not be of much help in dealing with the DOJ and SEC's exercise of their prosecutorial discretion to bring or refrain from bringing charges.
36. Rosenthal and Hanloser, at 2.
37. *See, e.g., Wilson v. Allstate Ins. Co.*, 785 F.2d 311 (6th Cir. 1986).
38. *In re March Rich & Co. A.G.*, 739 F.2d 834 (2d Cir. 1984).

© Deloitte Financial Advisory Services LLP, 2008. All rights reserved.

### **About the Author**

David F. Axelrod, a director in the Forensic & Dispute Services practice of Deloitte Financial Advisory Services LLP, specializes in FCPA and other corporate investigations. He is a former defense lawyer and Assistant U.S. Attorney, and has served as an adjunct professor at The Ohio State University Moritz College of Law.

David F. Axelrod  
Deloitte Financial Advisory Services LLP 155 East Broad St., 18th Floor  
Columbus, OH 43215  
Tel 614-228-4525  
Fax 614-233-6338  
daxelrod@deloitte.com