New York Law Journal
SERVING THE BENCH AND BAR SINCE 1888
Web address: http://www.nylj.com
VOLUME 235—NO. 98 MONDAY, MAY 22, 2006 ALM

LABOR & EMPLOYMENT LAW

A Multinational Bind

U.S. companies face legal and cultural clash over global codes of ethics and EU privacy policies.

BY MICHAEL STARR AND HANNO TIMNER

"BETWEEN the devil and the deep blue sea" may be the best way to describe the bind faced by American multinational companies as they try to comply both with U.S.-based pressures to maintain global codes of corporate ethics and with the privacy policies and philosophies of the European Union (EU). These conflicting cultural and legal norms clash headlong over the anonymous reporting of corporate wrongdoing—ranging from accounting fraud to sexual misconduct—which are favored by U.S. regulators and disdained by EU privacy policies.

In 2002, responding to the financial scandals at Enron, WorldCom and others, Congress enacted the Sarbanes-Oxley Act (SOX) which, in part, directs U.S.-based public companies to establish "procedures for the receipt, retention and treatment of complaints…regarding accounting, internal accounting controls or auditing matters."[1]

Significantly, those procedures must include mechanisms for "the confidential, anonymous submission by employees of concerns regarding questionable accounting or auditing matters."[2] Companies that do not comply with these requirements face severe consequences.[3] Moreover, implementing another provision of SOX, SEC regulations and the rules of self-regulatory agencies like NASDAQ and the New York Stock Exchange now require publicly listed companies to promulgate a corporate code of ethics, applicable to all employees, that not only sets ethical standards but also provides enforcement mechanisms that protect and encourage the reporting of questionable behavior.[4]

It is, however, not just SOX that matters. Federal sentencing guidelines for corporations place a high value on the adoption of compliance-inducing procedures, including corporate ethics codes that prohibit conduct that could violate U.S. criminal law—ranging from price-fixing to bribery of foreign officials.[5] Once again, mechanisms for confidential and anonymous reports of suspected wrongdoing are favored.[6] Add to this, U.S. employment discrimination law, which allows companies to avoid liability, or mitigate their exposure for damages, for such things as sexual harassment if they have in place preventive measures that, among other things, allow victims to come forward without fear of reprisal.[7] This is often understood to mean making an accusation with assurances that the accuser's identity will not be disclosed to the accused.

In response to this legal environment, virtually all major U.S. corporations have adopted company-wide codes of ethics that prohibit wide-ranging misconduct—far beyond "mere" questionable accounting—and encourage confidential or anonymous reporting of wrongdoing by employees of their co-workers or superiors. In addition, anonymous telephone "hotlines" are now common, which while virtually required for corporate audit committees to assure SOX compliance, are used for the full gamut of employee misconduct.

Applying what may be called the Mae West fallacy (Ms. West once having said, "Too much of a good thing is…wonderful"), U.S. companies naturally assume that their corporate codes of ethics, with their mechanisms for anonymous reports of wrongdoing, should be applied to their foreign subsidiaries. At least for SOX purposes, this may well be mandatory.[8] The practice, however, runs headlong into an entirely different set of cultural values and legal standards in Europe.

For countries in the EU, employment is

Michael Starr *and* **Hanno Timner** *are partners with Hogan & Hartson in the labor and employment group. They are resident in the New York and Berlin, Germany, offices, respectively.*

seen not simply as a contractual relationship that the employer can terminate at will (except for limited wrongful reasons) but rather as an entitlement or status relationship that needs to be protected from employer intrusion by, for example, ungrounded accusations of wrongdoing that could jeopardize an employee's standing or opportunity for advancement. This is coupled with EU privacy law—known as "data protection"—which limits how companies can collect, use and disseminate information about their own employees including—perhaps, especially—information suggestive of wrongdoing.

Wal-Mart Hotlines

The consequences of this culture clash was learned the hard way by the Wal-Mart Corporation when it was forbidden by the Higher Labor Court of Düsseldorf from implementing in Germany its corporate code of ethics, which included an anonymous telephone hotline.[9] The first mistake Wal-Mart made, according to the Düsseldorf labor court, was to implement its corporate ethics code unilaterally, without consultation with its "works council," which in Germany is a body collectively representing the interests of an employer's employees, even if there is no labor union.[10]

This would probably come as a shock to a typical U.S. corporate compliance officer, but many EU countries, like Germany, have mandatory "co-determination" laws that require companies to establish works councils and require that they be consulted on matters affecting employment.[11] Because Wal-Mart's ethics code sets standards for employee behavior, including rules that, if violated, could lead to discharge from employment, consultation with the works council in advance of promulgating the rule was, the High Labor Court held, required.

The Düsseldorf labor court also zeroed in on the portions of Wal-Mart's ethics code that banned any "romantic involvement" between employees of the company with co-workers who could have an influence on their professional development. In the United States, such provisions may be a protection against claims of sexual harassment.[12] But, according to the Düsseldorf labor court, that ethics rule violated the fundamental constitutional rights of Wal-Mart's employees to human dignity and personality, and it could not be adopted even if the company had complied with co-determination rules and obtained approval for the rule from its local works council.[13]

Personal Data

An even more intrinsic problem with the whistleblowing procedures adopted by U.S. corporations for purposes of SOX compliance is that, by their very nature, they require that employers collect, store and process data referring to employees of the company. Consequently, any actions taken in response to reports of misconduct will be deemed to relate to "personal data" within the meaning of EU data-protection laws and will require, among other measures, that the accused individuals be informed that such data is being "processed" about them, which could lead to their lawfully enforceable demand for access to that "personal data" for the purpose of correction.

Consequently, failure to tell the subjects of an anonymous allegation that their conduct is being investigated or to give them access to the "data" before the company's investigation is concluded could conceivably violate EU data-protection standards and might lead to sanctions, including severe administrative fines.

One more story tells this tale. In June 2005, McDonald's France and CEAC (a subsidiary of Exide Technologies) submitted their company policies on whistleblower hotlines to the French data protection authority, known as CNIL (Commission Nationale de l'Informatique et de Libertés). They were told that their planned ethics hotlines in units that operated in France were illegal.[14] The CNIL expressed a "reserve in principle" with regard to any system "whatever its form" that "organizes professional whistle blowing."[15]

According to the French data protection authority, the anonymous nature of the reports "encouraged wrongful or malicious accusations of criminal behavior" and individuals would be "stigmatized" as a result of an ethics report. The CNIL also objected because the "subjects" of the data compiled (i.e., the employees whose alleged wrongdoing is reported) would not know that data relating to their conduct was being collected, and would not have an immediate opportunity to access and correct the data at the time it was being "collected" against them.[16]

Quite apart from EU legal requirements, the CNIL's response to the anonymous hotlines clearly reflected heightened French sensitivity to confidential informants, arising from France's experience with the Vichy government during World War II when neighbors secretly reported on neighbors with dire consequences for real or concocted offenses.

Working Party Opinion

These decisions gave rise to ongoing public debate and led to the issuance of an opinion by the so-called "Article 29 Working Party" on Feb. 1, 2006, that was intended to provide guidance on how internal whistleblowing processes adopted to comply with SOX requirements could be implemented in a manner consistent with the EU's Data Protection Directive 95/46/EC (the Privacy Directive).[17] (The Working Party is a body established according to Article 29 of the Privacy Directive, whose main task is to provide guidance to the EU Commission and the general public on all relevant data protection issues. The Working Party is composed of members of each EU member state, usually the State Data Protection Commissioners.)

While the guidelines of the Working Party, such as its opinion regarding SOX whistleblower hotlines, are not legally binding, they are nevertheless adhered to by the national data protection authorities (like the French CNIL), which have participated in their drafting and issuance.

As a starting point, the Working Party points out that the implementation of internal whistleblowing procedures will, in the majority of cases, rely on the processing of "personal data" (i.e., the collection, registration, storage, disclosure and destruction of data related to identified or identifiable persons). This means not only that data protection rules are applicable, but also that both those individuals who file complaints or make claims through a hotline and also the accused individuals are entitled to rights under the Privacy Directive and corresponding provisions of member states' laws.

The Working Party also notes that for any processing of personal data to be lawful, the processing needs to be legitimate and satisfy one of the grounds set out in Article 7 of the Privacy Directive. As is relevant to corporate codes of ethics, the data processing must either be necessary for compliance with a legal obligation of the company or for a legitimate interest by the "controller" of the data (i.e., the employer) or by the third party to whom

the data is disclosed. Because the Working Party holds that an obligation imposed by a foreign legal statute or regulation, such as SOX, does not qualify as a "legal obligation" within the meaning of Article 7 of the Privacy Directive, anonymous whistleblower mechanisms could be lawful, the Working Party said, only if required by "principles of good corporate governance to ensure the adequate functioning of organizations."[18]

Fortunately for U.S. companies, the Working Party acknowledges that preventing fraud and misconduct in accounting, internal accounting controls, auditing and reporting, financial crime and insider trading appears to be compelling reasons to process personal data through a whistleblower process, though whether this extends to misconduct other than in accounting or securities, such as sexual harassment, was not addressed.

Developing a Process

The Feb. 1 opinion of the Working Party identifies specific ways for EU-based employers to develop a whistleblower process that complies with EU data protection requirements. One of the main concerns of the Working Party is the use of anonymous reporting mechanisms, which was also criticized by the French CNIL in the McDonald's case. The Working Party states that, in its view, anonymity is not an appropriate solution as it will be harder to investigate a concern if people cannot ask follow-up questions, and it may lead the investigation to focus on guessing who raised the concern. Anonymity also runs the risk of developing a culture of receiving anonymous malevolent reports, which, as the Working Party viewed it, would deteriorate the social climate within an organization.

Consequently, the Working Party explicitly demands that company policies discourage anonymous reports and, as an alternative, ensure that reports and the persons making reports are treated as strictly confidential. If, as an exception to the rule, anonymous reports are filed through a reporting system, such reports should, according to the Working Party, be subject to special cautionary measures and investigated and processed with greater speed than confidential complaints because of the risks of misuse.

Taking into account that SOX requires the implementation of procedures for the receipt of reports relating solely to "questionable accounting or auditing matters," the Working Party recommends that companies strictly limit data collected and processed in connection with reports and investigations to those facts necessary to verify allegations with respect to financial irregularities. If feasible, the companies that adopt whistleblowing procedures should limit the number of individuals entitled to report misconduct as well as the number of persons to whom anonymous hotline reports may be made.

Lastly, the Working Party suggests that all employees of a company should be fully informed about the existence, purpose and function of the company's whistleblower processes, including who receives reports, who has a right of access, correction and deletion, and what procedures exist for confidentiality and to protect those who make a report from retaliation. The Working Party also recommends that, provided there is no risk of jeopardizing an effective investigation, the accused employees should be informed of the facts they are accused of, who may receive respective reports, and how they may exercise their rights of access and correction.

It is possible to develop a whistleblower program that complies both with SOX and also EU data-protection law, but it is not easy.

Among the measures also recommended by the Working Party is maintaining specific internal processes for managing hotlines (including special training), and separating the whistleblower processes from other departments of the company, as well as limiting disclosure of reports to those who need to know. It also recommended that investigations be handled by local operations or local third-party service providers (e.g., law firms). As with all personal data collected in the EU, to the extent reports must be transferred outside the EU, adequate protections must be in place prior to the transfer.

Though the Working Party's recommendations may be far less pragmatic than an American-based compliance officer would have hoped for and more protective of employee interests than of the company's legally compelled interest to ferret out wrongdoing, it does give a glimmer of hope for navigating successfully between the devil and the deep blue sea. Yes, Virginia, it is possible to develop a whistleblower program that complies both with SOX and also EU data-protection law, but it is not easy.

Companies should also know that they enter treacherous waters when they cavalierly extend to their European affiliates corporate codes of ethics and anonymous hotlines that range beyond the subject matter of SOX, and simultaneously cover a multitude of other non-financial ethical issues (such as romantic involvements between their employees).

1. SOX §301(4), 15 U.S.C. §78j-1(m)(4).
2. Id.
3. See SEC Rule 10A-3 (requiring de-listing of companies not in compliance with SOX standards for audit committees).
4. See SOX §406, 15 U.S.C. §7264; SEC Release No. 33-8177; NASDAQ Rule 4350; New York Stock Exchange Corporate Governance Rules, §303A, para. 10.
5. See U.S. Sentencing Guidelines Manual §8B2.1.
6. See id. §8B2.1(b)(5)(C).
7. See *Burlington Indus. v. Ellerth*, 524 U.S. 742, 765 (1998) (avoidance of liability for sexual harassment by adoption for preventive measures); *Kolstad v. American Dental Ass'n*, 527 U.S. 526, 546 (1999) (employers who make good-faith efforts to prevent discrimination by implementing policies that detect and deter discrimination can avoid punitive damages).
8. Cf. *Carnero v. Boston Scientific Corp.*, 433 F.3d 1, 6, 9-10 (1st Cir. 2005) (discussing applicability of various SOX whistleblowing provisions to foreign-based subsidiaries of U.S. public companies).
9. See LAG Düsseldorf of Nov. 14, 2005, 10 TaBV 46/05.
10. See §1 Betriebsverfassungsgesetz (German Works Council Constitution Act).
11. See, e.g., Royal Decree of Nov. 27, 1973, Art. 25 (Belgium); Labor Code, Art. L 432-1 & L 432-2-1 (France); 1980 Statute of Workers, Art. 62 et seq. (Spain).
12. See B. Lindeman & D. Kadue, "Sexual Harassment in Employment Law," 421-22 (BNA 1992) (discussing anti-fraternization rules as preventive measure). See generally EEOC Guidelines on Discrimination Because of Sex, 29 C.F.R. §1604.11(f) ("employer should take all necessary steps to prevent harassment from occurring"); *Faragher v. City of Boca Raton*, 524 U.S. 775, 803 (1998) (vicarious employer liability for sexual harassment predicated on employer's "greater opportunity to guard against misconduct").
13. See German Constitution Arts. 1 & 2 (protecting human dignity and individual's right of personality).
14. CNIL, Decision Nos. 2005-110 & 2005-111 (May 26, 2005).
15. Id.
16. Id.
17. Article 29 Data Protection Working Party, Opinion 1/2006 on the application of EU data protection rules to internal whistleblowing schemes in the fields of accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crime of Feb. 1, 2006.
18. Id.