

# COMPLIANCE WEEK

A Weekly Newsletter On Corporate Governance, Risk And Compliance

## New EU Opinion Clouds Whistleblowing Plans

By Melissa Klein Aguilar — February 28, 2006

**I**n what could become a major headache for U.S. companies doing business overseas, a European advisory body says whistleblower systems and codes of conduct should be tailored to comply with each European nation's data privacy laws.

The pronouncement comes from the European Union's Data Protection Working Party, and stems from a similar move by French regulators last year. Known as Article 29 and released Feb. 1, the policy essentially says companies must respect each nation's data-privacy laws as they implement whistleblower hotlines or other measures that might give rise to anonymous reports of other workers' actions (see related documents and coverage at right).

Article 29 is only an opinion from the Working Party, and does not carry the force of law itself. But it sounds alarms for companies trying to craft whistleblower systems as required by the Sarbanes-Oxley Act, since its membership is comprised of data-protection agencies in EU member states and they do have the regulatory muscle behind them to impose fines or take other enforcement action.

"This is a compliance obligation on a pan-European basis," warns Mark Schreiber, a lawyer at Edwards Angell Palmer & Dodge and co-chair of the privacy matters practice of the World Law Group. That the EU issued guidance only three months after France did the same for its own nation indicates just how seriously European regulators consider the matter, he said.

"Many U.S. companies didn't take the time or effort to adapt their codes of ethics and whistleblower mechanisms to EU data protection principles," Schreiber says. What's more, he adds, many companies "may not be fully informed or compliant with EU data protection laws."

France's data protection agency, the Commission Nationale de l'Informatique et des Libertés, issued guidance in November saying all businesses must get government approval of their whistleblower schemes. That decision came after CNIL ruled that the whistleblowing hotlines of the French subsidiaries of two American companies violated French data protection laws (see extensive coverage above, right).

In its opinion, the Working Party said the proliferation of whistleblowing systems in 2005 underscored the difficulties companies may encounter trying to implement them. Many of the issues relate to the scope of issues allowed to be reported through internal whistleblowing schemes, while others relate to labor law. And while the functioning of whistleblowing schemes is provided for by law in some EU countries, the majority of them have no specific legislation or regulation on the subject.

Complicating matters for companies are the differing data-protection laws from nation to nation. For example, some countries require companies to get approval from the data protection authorities to implement a whistleblower hotline. In France, Sarbanes-related hotlines must be approved by the CNIL. In Germany, they must be approved by each company's Works Council.

### Country By Country

Because of such variances, "the whistleblower schemes envisioned by the Working Party opinion could be an operational nightmare for companies," says Richard Wolf, senior vice president and corporate compliance officer at Cendant Corp. To comply with the law, he says companies may need to set up separate whistleblower systems in each EU member state "in anticipation of certain types of calls that may or may not

come.” Wolf notes that helpline call volumes tend to be lower from European locations, most likely due to cultural reasons. He is also trying to organize a working group of American compliance officers to share strategies about how to handle the subject.

Schreiber expects that some countries, such as Great Britain and Ireland, won’t require approvals. Others “whose data schemes are a bit more severe,” however, probably will require approval.

“I think the French model [of online, speedy approval] is going to be adopted by other EU countries, but it’s a country by country issue,” Schreiber says. “U.S. companies will have to have more limited whistleblower schemes and codes of ethics in EU countries than they do in the U.S. if they want to take advantage of quick approvals, such as the one offered by the CNIL in France.”

Schreiber says there is “a fair amount of unhappiness in portions of the U.S. business community in having to adjust their codes [of conduct] at all.”

Still, he says, a number of U.S. companies are reviewing the language in their codes and deciding what the appropriate boundaries and scope ought to be, what the reporting mechanism should be, and who would receive these complaints.

### **Balancing Extremes**

The Working Party opinion “shows that the European data protection authorities recognize that this is a problem for U.S. companies due to the importance of complying with Sarbanes-Oxley,” says Tracy Gray, a partner at Hogan & Hartson in Boulder, Colo.

Gray says the opinion contains some ideas that “can be constructively used, such as limiting the number of people that can access a report.” The opinion also recommends a hotline that’s “not anonymous per se, but is confidential,” Gray notes. A name is associated with a report, but only those investigating the report will have access to it and will not be able to disclose it. “Putting that process in place is should be workable,” she says.

“This opinion symbolizes some flexibility by the EU,” Gray says. “It shows they’re willing to work with U.S. companies to implement their SOX [whistleblower] requirements.”

Wolf, however, says the restrictions the opinion place on how public companies can protect against fraud “are too broad, and may lead to undesirable results in the fight against the phenomenon of transnational fraud. EU member states are now free to adopt rules that could hinder the ability to uncover fraud and get critical information to regulators or shareholders outside the EU.”

The use of anonymous, confidential reporting systems for early fraud prevention and detection “is borne out of thoughtfully considered and time-tested compliance and ethics program best practices,” Wolf says. He cites a 2004 report by the Association of Certified Fraud Examiners, indicating that employee tips are the number one way companies learn of fraud in their organizations.

Wolf stressed the need for balance between the public interest in having early fraud prevention systems and protection of individual rights. “Under the Working Party opinion, individual rights to privacy seem to be the only consideration, whereas U.S. law is more focused on the public interest and the integrity of the market,” he says. “I don’t think we have that balance right on either side of the pond, and one extreme is not necessarily better than the other.”

---

### **RELATED RESOURCES:**

BNA International World Data Protection Report

Article 29 Data Protection Working Party

**Related Coverage:**

France OKs Online Approval Of Whistleblower Plans (Jan. 17, 2006)

French Agency Speaks Out On Whistleblower Programs (Dec. 13, 2005)

New International Guidance On Whistleblower Programs (Nov. 29, 2005)

Guidance Expected On SOX And Foreign Laws (Nov. 15, 2005)

Multinationals Find SOX Is Conflicting With Local Laws (July 19, 2005)