

## New Guidance on Whistleblower Hotlines in the EU

By Lisa J. Sotto, Christopher Kuner, and Aaron P. Simpson

Congress enacted the Sarbanes-Oxley Act ("SOX") in 2002 in response to a series of corporate scandals that diluted confidence in the U.S. financial markets. The law was intended to improve the accuracy and reliability of corporate disclosures and financial statements and to enhance the ethical standards and accountability of companies that are publicly traded on U.S. stock exchanges. SOX imposes compliance obligations not only on publicly traded companies in the United States, but also on non-U.S. entities listed on U.S. exchanges. While Congress made significant efforts in drafting SOX to ease potential legal conflicts in non-U.S. jurisdictions, in certain instances the law imposes compliance obligations on non-U.S. entities that conflict with local laws.

Last year, a conflict arose between SOX's mandate that audit committees of public companies establish whistleblower hotlines on the one hand, and data protection laws in the Member States of the European Union ("EU") on the other. In response to a groundswell of concern from companies forced to comply with both SOX and EU data protection laws, European data protection authorities and the EU Article 29 Data Protection Working Party have issued guidance that will allow companies to comply with both sets of laws.

### SOX'S WHISTLEBLOWER REQUIREMENTS

SOX's requirement that audit committees established by company

Boards of Directors develop whistleblower procedures is intended to provide employees with the opportunity to express concerns regarding questionable accounting or auditing practices without the fear of retaliation. Section 301 of SOX, codified in §10-A(m)(4) of the Securities Exchange Act of 1934 (the "Exchange Act"), requires that audit committees establish procedures for:

the receipt, retention, and treatment of complaints received by the issuer regarding accounting, internal accounting controls, or auditing matters; and the confidential, anonymous submission by employees of the issuer of concerns regarding questionable accounting or auditing matters.

The SEC's adopting release provides companies with a measure of flexibility in meeting this requirement, stating that §301 does not mandate specific procedures, but instead allows audit committees wide discretion in developing a suitable whistleblower system, given the particular circumstances. See Standards Relating to Listed Company Audit Committees, Exchange Act Release Nos. 33-8220, 34-47654 and IC-26001 (Apr. 9, 2003), 68 Fed. Reg. 18,788 (Apr. 16, 2003). Companies are free to decide who should receive complaints, how to ensure anonymity, and how to effectively communicate the existence of the system to employees. While there are numerous ways to comply with this requirement, companies typically have chosen to establish telephone hotlines or Web-based complaint systems.

### DATA PROTECTION IN EUROPE

Unlike the sectoral approach to privacy favored by U.S. lawmakers, privacy is considered a fundamental human right in Europe. An understanding of the exalted legal and cultural status of privacy in Europe is

required to fully understand the significance of data protection to European regulators. The EU Data Protection Directive (the "Directive") constitutes the basis for Member State data protection law. Generally, the Directive seeks to protect "personal data," which is expansively defined to include "any information relating to an identified or identifiable natural person." Directive 95/46/EC, art. 2(a), 1995 O.J. (L 281) 31-50. Under the Directive, companies may not process personal data unless the processing is subject to an enumerated exception. *Id.* at art. 7. Enumerated exceptions include instances where:

- the data subject has provided unambiguous consent;
- the company is required to process personal data to perform a contract to which the data subject is a party or to take steps requested by the data subject prior to entering into a contract;
- the company is required to process personal data to comply with a legal obligation; or
- the company, or third parties to whom the data are disclosed, must process personal data to pursue legitimate interests, except where such interests are overridden by fundamental rights and freedoms of the data subject that require protection under Article 1(1) of the Directive.

In addition to processing data, companies are restricted from transferring personal data except in very specific circumstances. There is a general obligation for companies to inform data subjects about the recipients of their data, including any person to whom the data are disclosed. See *Id.* at art. 10. Data subjects have the right to: 1) be notified before personal data are disclosed for the first

*continued on page 2*

## Whistleblower

continued from page 1

time to third parties, 2) object to the disclosure of their data to third parties, and 3) exercise these rights expressly offered to them. *Id.* at art. 14.

### THE CONFLICT

Last summer, the French data protection authority (the “CNIL”) addressed the implementation by French subsidiaries of U.S. companies of whistleblower systems designed to comply with SOX. Initially, two decisions by the CNIL restricted the use of anonymous whistleblower hotlines. See [www.cnil.fr/index.php?id=1841](http://www.cnil.fr/index.php?id=1841). In these decisions (involving McDonald’s France and Compagnie Européenne d’Accumulateurs, an affiliate of Exide Technologies), the CNIL indicated that the French Data Protection Act (the “Act”) governed employee whistleblower hotlines. See *Loi n° 78-17, 6 Janvier 1978, J.O., 7 Janvier 1978*, available at [www.cnil.fr/index.php?id=301](http://www.cnil.fr/index.php?id=301). Pursuant to the Act, both companies involved sought prior authorization from the CNIL to operate their whistleblower hotlines. In both cases, the CNIL refused to authorize the hotlines because of their discriminatory potential, despite a number of mitigation efforts made by the companies.

In its decisions, the CNIL expressed fear that the hotlines “could result in an organized system of workplace denunciations,” and stated that it had “reservations in principle” regarding such hotlines in light of the Act. Because the CNIL indicated that the hotlines could lead to erroneous or slanderous workplace denunciations, it held that the hotlines were

illegitimate. The fact that the whistleblower systems could have been used to report practices that were illegal pursuant to French law — and not only under U.S. law — did not impact the CNIL’s decision.

The CNIL also found that the hotlines were disproportionate given their purpose and could have the effect of stigmatizing employees. The CNIL pointed out that other means exist to meet the same goal of seeking compliance with law and company rules, such as: 1) employee training; 2) auditing of the company’s financial transactions and books; and 3) reporting violations to the labor inspectorate and other competent authorities. The CNIL took this position despite the fact that: 1) use of the hotlines was not mandatory; 2) suspected employees were granted substantial rights, such as being informed soon after violations were reported; and 3) suspected employees had ample opportunity to defend themselves.

The CNIL criticized the hotlines because a suspected employee would not receive notice of a complaint at the moment his or her data were processed (*ie*, when the complaint was made) and, therefore, the employee had no meaningful right to object to the processing of the data. The CNIL did not cite a specific provision of the Act upon which it based this finding.

### MEMBER STATE GUIDANCE IN RESPONSE TO THE CONFLICT

#### *The French Response*

After meeting with the SEC last year and recognizing the compliance conundrum created by its rulings, the CNIL agreed to issue concrete guidance that would allow entities subject to SOX operating in France to implement a confidential, anonymous whistleblower system and comply with French data protection law. In December, the CNIL rendered its “decision” document in which it set forth conditions that, if satisfied, would permit compliance with both SOX’s whistleblower requirements and French data protection law. Assuming an organization: 1) structures its hotline so it conforms with the conditions indicated in the decision document, and 2) sends the CNIL a “declaration” stating its com-

mitment to act in accordance with those conditions, the organization is automatically authorized to implement its whistleblower hotline in France. The conditions set forth in the decision document include:

- limiting the scope of a whistleblower hotline to internal controls in the financial, accounting, banking, and anti-bribery areas;
- requiring whistleblowers to identify themselves, except that an organization may receive an alert from any anonymous whistleblower if the organization does not encourage anonymity;
- collecting and processing facts that are strictly limited to areas that may be covered by the hotline (*ie*, financial, accounting, banking, and anti-bribery issues) or facts that concern the organization’s “vital interest” or “the physical or moral integrity of its employees”;
- requiring that whistleblower reports be communicated only to a group of individuals who are specifically responsible for handling whistleblower alerts;
- complying with legal requirements regarding the transfer of personal data to countries that are not considered to provide adequate protection;
- destroying or archiving “immediately” data that are deemed to be outside the scope of the whistleblower system or doing so within 2 months of the end of the investigation if no disciplinary action or legal proceedings are initiated;
- taking all necessary precautions to safeguard the data during collection, communication, and storage;
- handling the identity of the whistleblower in a confidential manner to prevent any retaliation;
- providing information to potential users of the whistleblower system including: 1) the entity responsible for the system, 2) the purpose and scope of the system, 3) the optional nature of the system, 4) that there are no consequences for using the system, 5) the recipients of reports, 6) that there are no consequences for not using the system, and 7) that abuses of the system

continued on page 3

---

**Lisa J. Sotto** is a partner in the New York office of Hunton & Williams LLP and heads the firm’s Privacy and Information Management Practice. She also serves as Acting Chair of the U.S. Department of Homeland Security’s Data Privacy and Integrity Advisory Committee. **Christopher Kuner** is a partner in Hunton & Williams’ Brussels office and leads the firm’s Global Privacy Practice. **Aaron P. Simpson** is an associate in the firm’s New York office, specializing in privacy and data security issues.

# Whistleblower

*continued from page 2*

- may result in disciplinary or legal action;
- notifying individuals incriminated through the whistleblower hotline as soon as the data are recorded (but not before measures to protect potential evidence have been taken); and
- permitting access to a data subject's personal information and allowing him or her to correct or suppress it, if appropriate.

Organizations seeking to ensure that their whistleblower systems comply with the CNIL's conditions have two options. First, as indicated above, they may certify their compliance with the decision document by visiting the CNIL's Web site and signing a certification stating that their system conforms to the conditions set forth by the CNIL. Alternatively, if an organization wants to implement a system that does not strictly conform to the conditions stated in the CNIL's decision document, the organization may submit a description of its whistleblower hotline to the CNIL for individual evaluation and authorization. Assuming the CNIL does not request additional information, it will review a request for individual authorization within 2 months of filing.

## **The Dutch DPA's Conditions**

In addition to the CNIL, the Dutch Data Protection Authority also recently published similar guidance in response to a number of requests from global companies. The necessary elements of an acceptable whistleblower hotline in the Netherlands include:

- limiting the processing to that necessary to serve the legitimate interests of the company;
- limiting the scheme to the reporting of questionable accounting or auditing matters or "substantial offences";
- transferring data reported via a whistleblower hotline to the parent company only in the case of substantial abuses that exceed the authority of the local entity;
- encouraging confidential, rather than anonymous, reporting;

- informing the data subject that a report has been filed about him or her not later than "the moment" the information is recorded (with very limited exceptions);
- informing employees about the existence, purpose, and operation of the whistleblower hotline, and the data controllers involved;
- using "specialized" departments within the company to manage the whistleblower hotline (and favoring the use of third parties to initially vet the reported information); and
- retaining personal information related to a report for no more than 2 months from the end of the investigation.

## **PAN-EUROPEAN GUIDANCE**

After being presented with the CNIL's guidance document at a late 2005 meeting, the Article 29 Data Protection Working Party issued guidance of its own in an effort to provide more clarity for companies operating on a Pan-European level. The Working Party published this document in February 2006 with the professed intention of providing guidance on "how internal whistleblowing schemes can be implemented in compliance with the EU data protection rules enshrined in the [Directive]." As a broad principle, the Working Party believes that any whistleblower hotline required by SOX in Europe must comport with EU data protection law. In practice, this means that the processing of personal information in connection with a whistleblower hotline must be:

- Legitimate and either: 1) necessary for compliance with a legal obligation or 2) established in pursuit of a legitimate interest. The Working Party has indicated that legal requirements related to accounting, auditing, and combating bribery in certain Member States are sufficient in this regard. In those Member States in which no such laws exist, the goal of ensuring financial security in international financial markets can justify processing pursuant to a whistleblower hotline.
- Proportionate, meaning that: 1) the number of individuals eligible to report alleged misconduct and to

be reported should be limited where possible, 2) anonymous reports should not be the rule, and instead should be used only in limited circumstances, 3) data collected should be limited to facts related to ensuring appropriate corporate governance, and 4) personal data processed in connection with a whistleblower hotline should be deleted within 2 months of completing an investigation, subject to limited exceptions.

- Conducted in accordance with clear and complete information about the scheme. Employers must inform data subjects about: 1) the existence, purpose, and function of the whistleblower hotline, 2) the recipients of the reports, and 3) the right of access, rectification, and deletion for reported persons.
- Focused on the data subject's rights without damage to the whistleblower's rights.
- Conducted subject to reasonable technical and organizational precautions to preserve the security of the data. The aim of the Working Party's guidance is to protect data from accidental, unlawful destruction or accidental loss, and unauthorized disclosure or access. In addition, employers should take appropriate measures to guarantee the confidentiality of the whistleblower's identity.
- Managed by a group dedicated to handling whistleblower reports and leading internal investigations. This group must be comprised of specially trained and dedicated individuals, limited in number and contractually bound by specific confidentiality obligations.
- Conducted in accordance with the Directive's data transfer requirements. Any personal information collected through the whistleblower hotline may be transferred outside the EU to a country deemed to have inadequate protection of personal information only if the recipient: 1) is a U.S. entity that participates in the Department of Commerce's Safe Harbor program, 2) has entered into a transfer (model) contract with the EU entity,

*continued on page 4*

---

## **Whistleblower**

*continued from page 5*

or 3) has binding corporate rules in place that have been duly approved by competent data protection authorities.

- Conducted in compliance with the Directive's notification requirements. EU Member State law may impose an obligation on employers implementing whistleblower schemes to obtain approval from

their data protection authority prior to implementation.

### **MANAGING A WHISTLEBLOWER**

#### **HOTLINE IN THE EU**

Global companies will need to manage the whistleblower issue on two levels — the local level and the Pan-European level. At both levels, companies required by SOX to implement whistleblower systems would be well advised to carefully adhere to guidance issued by local data protec-

tion authorities and the Article 29 Data Protection Working Party. The guidance issued by the Article 29 Working Party should take some pressure off of other data protection authorities to forbid such systems, as was originally feared after the CNIL issued its initial decisions. This is a rapidly evolving area that requires vigilance on the part of companies that are seeking to implement whistleblower hotlines in the EU.

—❖—

---