

## Whistleblower Programs: Challenges for Multinational Companies

*If you have any questions regarding the matters discussed in this memorandum, please contact the following attorneys or call your regular Skadden contact.*

**Dana H. Freyer**

New York  
212.735.2506  
dana.freyer@skadden.com

**Gary DiBianco**

London  
44.20.7519.7258  
gary.dibianco@skadden.com

**Pierre Servan-Schreiber**

Paris  
33.1.55.27.11.30  
pierre.servan-schreiber@skadden.com

**Matthias Horbach**

Frankfurt  
49.69.74.22.01.18  
matthias.horbach@skadden.com

**Katherine D. Ashley**

Washington, D.C.  
202.371.7706  
katherine.ashley@skadden.com

\* \* \*

*This memorandum is provided by Skadden, Arps, Slate, Meagher & Flom LLP and its affiliates for educational and informational purposes only and is not intended and should not be construed as legal advice. This memorandum is considered advertising under applicable state laws.*

Section 301 of the Sarbanes-Oxley Act of 2002 (SOX) created, among other things, a requirement that public company audit committees establish procedures for (i) the receipt, retention and treatment of complaints received by the company regarding accounting, internal accounting controls or auditing matters; and (ii) the confidential, anonymous submission by employees of the company of concerns regarding questionable accounting or auditing matters. Multinational companies that seek to apply their whistleblower procedures to employees residing outside the United States need to be mindful of certain critical local law differences that will impact how they design and implement these procedures.

In implementing the whistleblower requirements of Section 301 (and the stock exchange rules regarding codes of conduct), U.S. companies typically adopt comprehensive codes of conduct that include mechanisms for anonymously reporting accounting and other concerns or suspected violations of law. Companies with global operations face the difficult challenge of reconciling the SOX whistleblower requirements with applicable local laws, among them labor and data protection laws in the European Union. While Sections 301 and 806 of SOX focus on providing reporting mechanisms for employees and others to report wrongdoing and on protecting the whistleblower from retaliation, EU labor and data protection laws focus, in addition, on protecting the due process and other rights of the whistleblower's target. To further complicate the issue, in recent years, several EU member states have provided disparate guidance and views regarding compliance with SOX's whistleblower requirements. Therefore, U.S. companies with EU subsidiaries (and foreign private issuers who sell securities on a U.S. exchange) are challenged with maintaining a global whistleblower program that complies with SOX but does not run afoul of EU labor and data protections laws and guidelines.

Following a German labor court decision, and the issuance of guidelines by the data protection authorities of France<sup>1</sup> and the Netherlands, the European Union Data Protection Working Party adopted in early 2006 a nonbinding opinion (EU Opinion) on the application of EU data protection laws to whistleblower programs in the areas of accounting, internal controls, auditing matters, anti-bribery, banking and financial

---

<sup>1</sup> In May 2005, France's data protection authority, Commission Nationale de l'Informatique et des Libertés (CNIL), prohibited the implementation of two SOX-inspired whistleblower programs submitted for CNIL approval by affiliates of McDonald's and Exide Technologies. In an effort to address the conflict between French data protection laws and SOX Section 301 requirements, CNIL issued guidelines in November 2005 and a December 2005 binding "unique authorization decision," which, together with the guidelines, clarified CNIL's position on the implementation of whistleblower procedures in France. In addition, the French Labor Department recently issued a circular regarding whistleblower hotlines and codes of conduct which, among other things, confirms the requirements regarding implementation of whistleblower programs under French labor laws, *i.e.*, that companies must (i) inform and consult with their works councils/employee representatives (as applicable) prior to implementation of such programs, and (ii) provide certain information to employees about such programs.

crimes.<sup>2</sup> The EU Opinion was intended to provide guidance on how a whistleblower program can be implemented in compliance with the EU Data Protection Directive (Directive), a template set of data protection rules used by EU member states to enact their own data protection legislation.<sup>3</sup> Among the Directive's key concepts are (i) personal data must be processed fairly and lawfully, be collected for specified, explicit and legitimate purposes, and not be used for illegitimate purposes; (ii) there should be proportionality between the data processed and the purpose for which it is collected; and (iii) procedures should be in place to ensure that inaccurate or incomplete data is erased.

Since the EU Opinion was adopted, Ireland, Luxembourg, Germany, Belgium and Spain have taken positions on whistleblower hotlines.<sup>4</sup> EU member states that have not yet established specific hotline guidelines will likely rely on the EU Opinion — subject, however, to each member state's interpretation. Therefore, when implementing global whistleblower programs, multinational companies must take into account the various interpretations that exist among different countries' guidelines. For example, SOX requires a hotline for reporting concerns regarding accounting, internal controls and auditing matters, but does not prohibit having a hotline for reporting other matters, such as employment concerns, theft in the workplace or other policy violations. In the EU, however, the subject matter that may be reported on a whistleblower hotline is limited to varying degrees by member states. Additionally, the availability of an anonymous reporting mechanism is required by SOX (at least for accounting- and auditing-related concerns) but is frowned upon in France and is prohibited in Spain, thus causing a direct conflict for companies that are subject to SOX and have employees in Spain. EU member states also differ on whether the data protection authority of a given EU member state must be notified of the hotline or approve the hotline before it is implemented. For example, France decided to combine these two approaches, with a two-level regime, requiring a company to: (i) provide a unilateral undertaking for whistleblower systems that comply strictly with the content of the CNIL's 2005 unique authorization decision; or (ii) request prior authorization from the CNIL if the company wishes to implement a system that is not totally compliant with the unique authorization decision.

So how can a multinational company structure a whistleblower program that complies with the requirements of Sarbanes-Oxley, on the one hand, and the requirements of the jurisdictions of its EU operations, on the other hand? The goal should be to create a whistleblower system that is responsive to the EU Opinion's guidelines and local law requirements, complies with Sarbanes-Oxley and achieves the compliance objectives of facilitating the reporting of legal and ethical concerns and violations. Because regulations and judicial guidance in the European Union continue to evolve in this area of law, there is currently no simple solution. However, several approaches have emerged that can be tailored to a company's specific locations and operations. First, though it may be administratively and logistically easiest to establish one global hotline that accommodates all applicable laws, this

---

2 The "Article 29 Data Protection Working Party" is an independent advisory body established to provide expert opinion on questions of data protection, to promote the uniform application of the general principles of the EU Data Protection Directive in all member states and to make recommendations to EU institutions on matters of data protection. The EU Opinion can be found at: [http://europa.eu.int/comm/justice\\_home/fsj/privacy/docs/wpdocs/2006/wp117\\_en.pdf](http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2006/wp117_en.pdf).

3 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995, OJ L 281, 23.11.1995, p.31, available at: [http://ec.europa.eu/justice\\_home/fsj/privacy/docs/95-46-ce/dir1995-46\\_part1\\_en.pdf](http://ec.europa.eu/justice_home/fsj/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf).

4 See Donald C. Dowling, Jr., "Sarbanes-Oxley Whistleblower Hotlines Across Europe: Directions Through the Maze," 42 THE INT'L LAWYER 1, 32-37 (2008) for a description of, and citations for, the nonbinding positions taken by these EU jurisdictions. In the United Kingdom, the Public Disclosure Act of 1998 was adopted to provide protection from retaliation to employees who blow the whistle on wrongdoing. However, the UK has not yet issued any formal views relating to the impact of UK data protection laws on SOX-compliant hotlines.

results in a very broad, general hotline that can contain only the “common denominators” of each jurisdiction. Second, and more targeted, some companies are establishing separate hotlines for their EU and non-EU employees. This approach allows the non-EU hotline to include U.S.-type restrictions and requirements on non-EU employees. Even under this approach it is important to reconcile the EU hotline with the EU Opinion and the disparate guidelines of the EU member states and of each country in which a company conducts business. Third, companies can design separate hotline structures for EU and non-EU employees, and further tailor the EU hotline to the requirements of each EU jurisdiction of operation. Under this approach, the hotline operating in the United States and other jurisdictions, where permissible can maintain the “US best practices approach” while employees in specific EU jurisdictions have access to a hotline that is tailored to local requirements. This approach can be implemented by providing country-specific telephone numbers and publishing local policies describing the specifics of the hotlines. Although it is more cumbersome to implement than the more general approaches, tailoring the hotline to specific jurisdictions provides companies with the benefit of a U.S.-type hotline where permitted, while following local guidelines where necessary.