

International HR Best Practices Tip of the Month

January 29, 2010

This Month's Challenge

Broad corporate codes of conduct, with anonymous whistleblower hotlines, have become increasingly popular, but may not be compliant with French data protection requirements.

Best Practices Tip of the Month

A recent decision by the French Supreme Court casts further doubt on the viability of whistleblower hotlines in France. To meet French legal requirements, consider a narrowly drawn whistleblower program.

French Supreme Court Limits the Scope of SOX Whistleblowing Procedures

The Sarbanes Oxley Act requires covered companies to implement procedures for “the confidential, anonymous submission by employees of . . . concerns regarding questionable accounting or auditing controls” and mandates protection of whistleblowers from retaliation. Driven, at least in part, by this legal obligation, many companies have adopted broad codes of conduct, specifying a host of legitimate corporate concerns (for example, compliance with anti-bribery, antitrust, environmental, employment and other laws and regulations) and setting up hotlines to field anonymous complaints and tips that might lead to the discovery of wrongdoing within the company.

The implementation of these codes of conduct and whistleblower hotlines is expanding at the international level, but global companies must pay attention to local law requirements when rolling out these codes in foreign countries, where strict data protection laws, largely absent in the United States, may bar the company from inviting or processing anonymous allegations and charges.

A recent decision by the French Supreme Court provides a good illustration of issues that may be raised by local laws in the implementation of whistleblowing procedures abroad. For the first time, the French Supreme Court addressed the issue of the validity of a code of conduct that had been implemented by a listed company (*Dassault Systèmes*, a French software company) in order to comply with the Sarbanes Oxley Act.

In its December 8, 2009 decision, the French Supreme Court overruled the decision of the Court of Appeal, which had declared the whistleblowing system implemented in the code of conduct of *Dassault Systèmes* compliant with the requirements imposed by the French data protection authority (CNIL) and therefore legal.

This was not the first time that a multinational company's whistleblower policy had run afoul of French data protection law. In a landmark decision rendered in 2005, the CNIL declared that the broad and anonymous whistleblowing procedures of several companies, including McDonald's Corporation, that had been adopted in order to implement the requirements of the Sarbanes Oxley Act, were contrary to French law and in particular to the French data protection law of January 6, 1978. The CNIL held that it had no fundamental objection to that kind of system, but it expressed the opinion that whistleblowing processes should not be transformed into an organized system of professional denouncement that could jeopardize the rights of the accused employees.

In order to reach a compromise between SOX requirements and French law, the CNIL issued a formal *Délibération* on December 8, 2005. The *Délibération* states that companies are authorized to roll out their whistleblowing systems provided they formally disclose the existence of the system and they comply with the requirements of the *Délibération*. In particular, Article 1 of the *Délibération* authorizes companies to adopt whistleblowing systems implemented in response to French legislative or regulatory internal control requirements (for example, regulations governing banking institutions) or the whistleblowing requirements of the Sarbanes Oxley Act. Article 3 of the *Délibération* provides that alleged wrongdoing that is not encompassed within these core areas may be covered by the whistleblowing system only if vital interests of the company or the physical or mental integrity of its employees is threatened.

If the scope of the whistleblowing process exceeds that authorized by the CNIL's *Délibération*, the company is under the obligation to enter into a burdensome approval process with the CNIL, which requires the company to provide detailed disclosure concerning the information to be collected, the recipients of the information, and the end-purpose for which the data will be used. So far, the CNIL has never given its authorization when the scope of the whistleblowing system exceeds its *Délibération*.

In the case at hand, Dassault had implemented a whistleblowing system, and a trade union challenged the validity of the system on the grounds that the company should have sought a formal authorization from the CNIL, because its scope exceeded auditing and financial matters.

The Supreme Court ruled that the scope of Dassault's code of conduct was too broad, in that it invited employees to report violations relating to more than just finance, accounting and anti-corruption matters, including intellectual property rights, confidentiality, conflict of interest, discrimination, and sexual or psychological harassment.

It ruled that the Dassault code of conduct's whistleblowing scheme was invalid because it permitted whistleblowers to report on alleged violations of company policies other than those enumerated under Article 1 of the CNIL *Délibération*. According to the Court, a whistleblowing system that would allow complaints concerning other breaches of the code of conduct besides those listed must be authorized specifically by the CNIL on a case-by-case basis. Even though these breaches are material and might threaten the vital interest of the company or the physical or mental integrity of its members, the Court determined that case-by-case review was required.

The Supreme Court also found that Dassault's Code of Business Conduct was defective because it did not expressly state that the individuals accused of wrongdoing had the right to access the information reported, and a right of correction where the information was not correct.

From a practical point of view, there is a strong likelihood that the CNIL will refuse to grant an authorization for a whistleblowing system exceeding the scope of the CNIL's *Délibération*, so multinational companies may end up restricting their whistleblowing systems to the core areas specified in the CNIL's *Délibération* of December 8, 2005 to avoid their procedures being invalidated.

Related Professionals

- **Howard Z. Robbins**

Partner

- **Anthony J. Oncidi**

Partner