

## Decision Issued on Implementing Sarbanes-Oxley Whistleblowing Procedures in France

January  
2006

France has recently adopted a decision aimed at resolving a conflict of laws facing companies with operations in France subject to the Sarbanes-Oxley Act (the Act). This briefing explains the conflict that gave rise to this decision, its substantive scope, and the related labor law considerations.

### **Anonymity vs. Individual Privacy Rights**

In France, Sarbanes-Oxley-compliant whistleblowing procedures have posed legal conflicts because the anonymity required by the Act raises concerns under French and European Union regulations that protect the rights of individuals accused of violations. A cornerstone of the enhanced financial reporting envisaged by the Act is the requirement that audit committees of companies subject to the Act establish procedures for the “confidential, anonymous submission by employees of the issuer of concerns regarding questionable accounting or auditing matters.” In addition, the Act provides protection to whistleblowers by making it a criminal offense to retaliate against any person, including interference with that person’s lawful employment or livelihood, for providing truthful information to a law enforcement officer relating to the commission or possible commission of any U.S. federal offense. This extension of protection to persons reporting a broad range of possible offenses inspired a number of companies to propose whistleblowing procedures that went beyond the strict minimum of “questionable accounting or auditing matters” and included procedures for reporting on environmental, health and safety, and other matters.

The processing and recording of anonymous complaints raises privacy concerns with respect to the accused under the French Data Protection Act of January 6, 1978, as amended, and the European Union Directive on Data Protection, Directive 95/46/EC of October 24, 1995. These data protection rules provide individuals with specific rights when data relating to them are being processed: the right to a fair collection process, the right to be informed of the fact that data is being collected, the right to object to the collection, and the right to correct erroneous information.

The French Data Protection Authority, or Commission nationale de l’informatique et des libertés (CNIL), is responsible for enforcing these rights. Automated systems for processing personal data, including anonymous whistleblowing procedures, must be either formally declared to, or authorized by, CNIL. Where systems are implemented without proper notification to CNIL, criminal sanctions in the form of imprisonment and fines can be imposed.

In May 2005, CNIL issued two decisions refusing to authorize Act-compliant whistleblowing procedures by the French subsidiaries of two U.S. public companies, McDonald’s and Exide Technologies. The decisions focused on the risk of abusive reports of violations and called into question the necessity of anonymous reporting in light of various existing procedures under French law, including internal and external audit processes and the possibility of reporting violations to competent governmental authorities.

Over the following six months, CNIL conducted an informal consultative process. On November 10, 2005, CNIL published guidelines for anonymous complaint procedures that would comply with French and EU law while satisfying the requirements of the Act. In late December 2005, CNIL published a formal decision dated December 8, 2005 setting forth conditions for a simplified authorization procedure. Rather than undertake a prior authorization procedure, companies may now formally declare to CNIL that the whistleblowing procedures they wish to implement comply with the criteria set out in the decision. Where whistleblowing procedures do not fulfill such criteria, they must be authorized by CNIL prior to their implementation.

### **Substantive Scope of the CNIL Decision**

In order to discourage abusive or disproportionate complaints, Article 1 of the decision limits the scope of anonymous procedures to those that are required by French law, namely, those related to finance, accounting, banking, and anti-corruption.

Act-compliant whistleblowing procedures fall explicitly within the scope of the decision. Whistleblowing systems will benefit from the simplified procedure, provided that they comply with these standards laid out in the decision:

- ♦ Whistleblowers must identify themselves, and the company must ensure that a whistleblower's identity remain confidential. The company may, however, collect information that was submitted anonymously where (1) the processing of the complaint has built-in safeguards such as a preliminary evaluation, and (2) the company does not encourage use of the anonymous procedure, but rather, the procedure encourages employees to identify themselves.
- ♦ Personal data that may be processed is limited to: (1) the whistleblower's identity, position, and address; (2) the accused person's identity, position, and address; (3) the identity, position, and address of the persons involved in the data gathering or in the whistleblowing procedure; (4) reported acts; (5) information gathered during investigation; (6) the investigation report; and (7) additional information given after the initial complaint. Furthermore, all information must be objective, necessary to the investigation, and fall within the type covered by the whistleblowing procedure.
- ♦ Only specialists who have a contractual obligation of confidentiality should have access to the reports. Employees who are authorized to access personal data may only do so to the extent necessary. If a company outsources reporting to a service provider, access to personal data is limited to the service provider's scope of duties. By contract, service providers must not use information for illegitimate purposes, must ensure confidentiality, and must respect the time limits for retention as well as ensure destruction or restitution of all support manuals or personal information when their services end.
- ♦ Companies may transfer personal data to U.S. companies that are certified by the EU/U.S. safe harbor process and that have expressly included human resources information within the scope of their privacy policies. Under the safe harbor approach, U.S. companies can certify to the U.S. Department of Commerce that they meet certain criteria and provide "adequate" privacy protection for personal data.
- ♦ Information that falls outside the scope of the whistleblowing procedure must be immediately destroyed or archived. Companies should not store reports for more than two months following the close of an investigation, unless disciplinary proceedings have been initiated. When disciplinary or judicial proceedings take place against the accused or a whistleblower lodging an abusive complaint, information should be stored until the close of proceedings. An independent storage system with limited access should be created for the duration of the proceedings.
- ♦ Companies must take all measures necessary to protect the security of the information throughout processing and storage. Authorization mechanisms such as logins and password protection should be used. Access to data systems should be registered and regularly controlled.
- ♦ Companies are to provide clear and complete information on the procedure, identifying in particular: the entity responsible for the system, the objective sought and the subjects that may be covered by the complaints, the optional nature of the system, the absence of consequences for employees for not using the system, the recipients of the alerts, the eventual transfer of the information outside of the European Union, as well as the existence of a right of access and rectification for persons accused. Abuse of the system may result in disciplinary action and judicial proceedings against the whistleblower. Use in good faith, even if the allegations are not subsequently substantiated, will not subject the whistleblower to sanctions.
- ♦ The accused should be notified and should have an opportunity to correct errors in the report. Notification may be delayed if necessary to prevent destruction of evidence.
- ♦ All persons identified by the whistleblowing procedure have the right to access information regarding them and to correct or suppress incomplete, incorrect, ambiguous, or outdated information. In no case will the accused be able to learn of the identity of the whistleblower.

## Labor Law Considerations

In addition to data protection concerns, implementing whistleblowing procedures raises issues under French labor law.

Because implementation of a code of conduct containing whistleblowing procedures would ordinarily modify the system by which a company records personal data about its employees, a company is required to inform its workers' representative, ordinarily the workers' council (comité d'entreprise).

In addition to this notification, a company may wish to consider amending its existing workplace rules (règlement intérieur) to expressly include a code of conduct. Amending the existing rules would reduce legal risks related to the implementation of the procedures, and ensure that such procedures are enforceable against all employees.

The workers' council also must approve the implementation of an anonymous complaint procedure. A recent decision against BSN Glasspack, a French subsidiary of Owens-Illinois, regarding its implementation of a Sarbanes-Oxley-compliant toll-free "ethics hotline" effectively requires such approval. In *BSN Glasspack*, a French court awarded a workers' council and workers' union nominal damages, finding that the company had violated labor law by posting on the company bulletin board two notices concerning the toll-free "ethics hotline" after having only "simply informed" the workers' council of the implementation of the anonymous complaint procedure.

As for enforceability, under French labor law it is not possible to require employees to sign the whistleblowing procedures. Nevertheless obtaining signatures voluntarily could enhance the company's position in any future dispute, specifically with regard to the transfer of personal data to the United States. Amending the workplace rules to include the procedures would make them enforceable against all employees and reduce the risk that an employee who refused to sign the procedures voluntarily could challenge the legitimacy of a future disciplinary proceeding arising from an anonymous complaint.

This Sarbanes-Oxley Act briefing also is available on the Winston & Strawn website at [www.winston.com](http://www.winston.com). Please look under the Publications heading at the top of the home page, then click on the Sarbanes-Oxley Act Info link in the left-hand navigation bar to access the briefing.

If you have any questions about the matters contained in this client briefing, please call your usual contact at Winston & Strawn or any of the following attorneys:

### In Paris

*Corporate*  
Paul Bishop  
(33 1) 53 64 82 01  
[pbishop@winston.com](mailto:pbishop@winston.com)

Alexandre Brue  
(33 1) 53 64 82 17  
[abrue@winston.com](mailto:abrue@winston.com)

Robert Flanigan  
(33 1) 53 64 82 51  
[rflanigan@winston.com](mailto:rflanigan@winston.com)

Jérôme Herbet  
(33 1) 53 64 82 04  
[jherbet@winston.com](mailto:jherbet@winston.com)

Vincent Trevisani  
(33 1) 53 64 81 84  
[vtrevisani@winston.com](mailto:vtrevisani@winston.com)

*Labor and Employment*  
Sebastien Ducamp  
(33 1) 53 64 82 08  
[sducamp@winston.com](mailto:sducamp@winston.com)