Paul Hastings

March 2006

StayCurrent

A Client Alert from Paul Hastings

New French Whistleblowing Self-Certification Regulations

Since Congress enacted the U.S. Sarbanes-Oxley Act ("SOX") in 2002 following the Enron and WorldComm debacles, audit committees of U.S. listed companies have been required to establish "whistleblowing" procedures[1] enabling employees to make anonymous, confidential reports and complaints regarding questionable accounting, internal accounting controls, or auditing matters.[2] In response to SOX, many U.S.-based multinational companies complied with SOX by implementing anonymous whistleblowing "hotlines" world-wide. Some of these whistleblowing procedures, however, have run afoul of non-U.S. employment and privacy laws, particularly in the European Union (the "EU"), where data privacy protection standards are much higher than in the United States.

The French National Processing and Liberties Commission ("CNIL")[3] made this data privacy concern abundantly clear in May 2005, when it refused to authorize whistleblowing procedures that the French subsidiaries of McDonald's Inc. and Exide Technologies had submitted for approval.[4] CNIL declared that the procedures violated French privacy laws primarily because of both the anonymity of the hotlines and the broad scope of matters that could be reported. CNIL's decisions left many U.S.-based multinational companies operating in France uncertain as to how to comply both with SOX and French privacy law.[5]

In an effort to eliminate this confusion, CNIL issued "guidance" on the whistleblowing question ("Guidance") on November 10, 2005 that a whistleblowing procedure could be implemented "only for voluntary use" by employees and only as a "supplement [to] other means of communication" within the company. According to the Guidance, ***the ordinary method for reporting company-related issues should be to senior management, through normal reporting channels, or by open lines of communication involving employee representatives or statutory auditors.*** While the Guidance gave companies some direction, it was limited and left important issues unresolved.

The good news for U.S. multinational companies is that CNIL resolved most of the remaining issues on December 28, 2005, when it issued a whistleblowing directive (the "Directive"). The Directive permits companies to self-certify SOX whistleblowing procedures that meet the Directive's precise requirements. This client alert describes those requirements and recommends how to structure SOX whistleblowing procedures to minimize potential exposure under the EU privacy laws.

Brief Summary of the Directive

A self-certified whistleblowing procedure must meet the following requirements:

- *Scope.* The whistleblowing procedure should be limited to meeting French legal requirements for financial institution internal controls or for accounting or anti-corruption purposes. A whistleblowing procedure designed to comply with SOX requirements is permissible only to the extent it satisfies this requirement.

- *Non-Anonymous Reporting.* A whistleblowing procedure must encourage non-anonymous reporting. ***In fact, CNIL officials informally have advised us that no communication to employees should reference the ability of whistleblowers to submit anonymous reports.*** The staff of the U.S. Securities and Exchange Commission (the "SEC") informally has advised us that it believes that a company should be permitted to publicize the existence of an anonymous procedure. At this time, however, the SEC has not commented formally on this aspect of the Directive.

- *Whistleblower Confidentiality.* The identity of any whistleblower, anonymous or not, must be kept confidential, so that the whistleblower does not suffer retaliation as a result of proper, nonabusive whistleblowing.

- *Communications Regarding the Procedure.* A company must describe a whistleblowing procedure's significant features, including:

  - why it was implemented;
  - who may use it;
  - who administers it;
  - who receives whistleblowing reports;
  - its purely voluntary nature and the lack of any penalties for nonutilization;
  - the right of accused persons to correct erroneous information;
  - that improper or abusive whistleblowers may be disciplined or be subject to legal action; and
  - how the data concerning the whistleblower, the accused, and the accusation will be protected outside the European Economic Area (the "EEA") in countries that do not provide adequate data protection under the EU Directive on Data Protection (the "EU Directive") (as discussed below).[6]

- *Processing Requirements.* A report may be accepted only after its first recipient conducts a preliminary analysis with respect to whether the report should be processed. The first recipient may process a report only to the extent that it (i) is objective, (ii) is within the scope of the whistleblowing procedure,[7] and (iii) contains only information that is strictly necessary to verify the facts alleged. Generally, the following are the only categories of data that may be collected as a result of a whistleblowing report:

  - The identity, responsibilities and contact information of the whistleblower, the accused, and the persons processing the whistleblowing report;
  - The allegations;
  - Information verifying the allegations or about the verification process (*e.g.,* interview of relevant individuals, study of relevant files, transaction records); and
  - Follow-up and further steps with respect to the report.

  For example, if a whistleblower accuses a senior officer of an accounting fraud and marital infidelity, the marital infidelity accusation must be ignored and deleted from the whistleblowing records.

- *Persons Handling Reports.* Whistleblowing reports should be handled by the smallest number of persons practicable, and each of them must be properly trained and must have signed a strict confidentiality agreement.

- *Cross-Border Whistleblowing.* French employees' whistleblowing reports may be processed outside of France. If they are processed in a non-EEA country that does not provide data protection adequate to satisfy the EU Directive, the processors must undertake one of the measures provided by the EU Directive to achieve adequate data protection.[8] ***The EU has deemed the United States to have inadequate data privacy protection.***[9] In most cases, the whistleblowing report must be sent to personnel in France for investigation.

- *Disclosure of Reports.* Whistleblowing reports must be kept confidential except to the extent disclosure is necessary. Disclosure is permissible in the following situations, among others:

  - *To Company or Company Affiliate Personnel*—to the extent disclosure is necessary to an investigation, but only if in compliance with French data privacy protection laws or the alternatives discussed above under the heading "Cross-Border Whistleblowing."
  - *To a Whistleblowing Procedure Outsourcer*—if the outsourcer is bound contractually (i) not to use any information obtained for improper purposes, (ii) to ensure the confidentiality of the information, and (iii) to retain any such information only for a limited period of time (as discussed below).

- *Retention and Disposal of Reports.* A whistleblowing report deemed to be groundless or outside the scope of permissible subjects for whistleblowing reports should be destroyed promptly. Otherwise, a whistleblowing report should be destroyed or archived within two months following the termination of any verification efforts, except where action is taken against the person targeted in the report or the whistleblower.[10] If action is taken, the report may be retained during the investigation and any resulting proceedings. Retained information and data must be kept separate from active whistleblowing reports and must be protected with additional safeguards (such as a special password) to limit access. The maximum retention period is the period for bringing legal action related to the subject of the complaint (*i.e.,* the relevant statute of limitations period).

- *Prompt Notification and Rectification Rights.* An accused person should be advised as soon as the whistleblowing report is received but only after proper measures have been taken to protect the evidence. The notification must state who is handling the report, who has received the report, the facts alleged, and data access and correction rights. The identity of the whistleblower, however, must not be disclosed. The person also must be provided with the information about the whistleblowing procedure (see "Communications Regarding the Procedure" above), if he or she has not already received such information. The person may request correction or deletion of any erroneous information.

Action Plan

We recommend that all affected companies consult French and U.S. legal counsel to determine whether the Directive will require them to change their whistleblowing procedures, codes of conduct and ethics, or any other company policies and regulations. The consequences of Directive non-compliance include shutting down the whistleblowing procedure, fines, and penalties.

Accordingly, we recommend that employers use this compliance approach:

- *Ensure the Whistleblowing Procedure Is a Supplemental Means of Communication.* A whistleblowing procedure used in France should supplement an effectively functioning system of direct, non-anonymous reporting of illegal, unethical, or other problematic activities. De-emphasizing the role of a supplemental whistleblowing procedure should be consistent with SOX.

- *Comply with the French Data Privacy Laws and, if applicable, the EU Directive.* To the extent that whistleblowing reports are received and processed only France, comply with French data privacy laws. As to cross-border whistleblowing reports made from France to recipients in a non-EEA country, the data protection requirements of the EU Directive must be met.

- *Limit the Whistleblowing Procedure's Scope to Accounting and Auditing Matters.* Scale back the scope of the procedure to meeting SOX requirements only to the extent they are consistent with any of the purposes the Directive permits.

- *Train Personnel.* Train personnel who monitor the procedure, receive and process whistleblowing reports, or who act on them about the requirements of the Directive and Guidance. The core team should be small enough so that the company can supervise it effectively, and each team member should execute special confidentiality agreements.

- *Review Outsourced Whistleblowing Procedures.* Ensure the outsourcer understands the Guidance, Directive, and SOX obligations. Because the employer remains responsible for Guidance and Directive compliance, make sure that outsourcers promise to comply and agree to indemnify the employer if they do not. Employers should monitor outsourcers to ensure compliance.

- *Process Whistleblowing Reports in an EEA Country.* An employer should process[11] whistleblowing information within the EEA to the fullest extent possible.

- *Communication to a non-EEA Country Audit Committee.* If the audit committee is located outside the EEA, determine in the EEA whether to release whistleblowing information to it. Be careful not to obstruct paths of communication to the audit committee in an effort to retain information within the EEA.

- *Export of Information Outside the EEA.* If a company needs to transfer information from France to any non-EEA jurisdictions that do not provide adequate data protection for purposes of the EU Directive (*e.g.,* the United States), transfer it in compliance with the EU Directive.

- *Self-Certification of a Whistleblowing Procedure.* Audit the whistleblowing procedure periodically for Directive and Guidance compliance.

- *Consult with Works' Councils.* Consult with works' councils or employee representatives before implementing a new whistleblowing procedure in France. The French Ministry of Labor, whose jurisdiction covers employment matters (rather than data protection) is expected to release guidance on whistleblowing procedures in the near future.

Other European Jurisdictions

Similar whistleblowing issues exist in all other European jurisdictions, such as these:[12]

Italy

Italy does not have any law or regulation that authorizes or requires companies to implement whistleblowing procedures. Whistleblowing procedures must comply with Italian law, in particular, the Italian Civil Code, the Italian Criminal Code, the Italian Labor Law (in particular, Law n. 300 of May 20, 1970 and the National Collective Labor Agreements) and the Italian Law on Data Protection (Law n. 196 of June 30, 2003). Italian courts have not issued any whistleblowing-related rulings under any of these laws, nor has the *Garante della Privacy,* the agency that monitors privacy law compliance, provided any specific guidance. Given the similarities between the Italian and the French data protection laws, significant parts of which are derived from the EU Directive, a company in Italy should assume that any whistleblowing procedure should be implemented in accordance with the principles highlighted by CNIL.

United Kingdom

Likewise, there is no United Kingdom analog to the Guidance or Directive, but the U.K. Information Commissioner's office has confirmed that they are largely consistent with evolving U.K. data privacy principles, particularly their emphasis on (i) limiting the scope of whistleblowing procedures, (ii) discouraging anonymous reporting, and (iii) making whistleblowing

procedures supplemental to more normal internal communications processes.

In other respects, however, the data protection regime in the United Kingdom is more company-friendly than is the French model. For example, the U.K. Employment Rights Act 1996 provides that qualifying disclosures for the purposes of whistleblowing protections include those relating to miscarriages of justice, health and safety concerns, criminal offences generally and environmental risks. This list of permissible subject matters is not exhaustive, and contrasts sharply with the very limited list under the Directive. The overarching principle used to determine the permissibility of a whistleblowing procedure in the United Kingdom is whether it is proportional to the magnitude of, or threat posed by, the issue that is intended to be addressed. The generally held view in the United Kingdom is that whistleblowing procedures are to be welcomed as providing a helpful alternative to silence, on the one hand, and monopolistic control of information by managers, on the other.

Notes:

1. A whistleblowing procedure allows employees to report allegations of illegal or unethical activities or breaches of company policies or regulations to parties outside the normal reporting channels. While an employee typically would communicate any workplace issues to his or her supervisor, if the issue is of a type that the employee cannot comfortably disclose to the supervisor (*e.g.,* fraud committed by the supervisor), the whistleblowing procedure would provide an alternative means by which the employee can report the issue.
2. *See* 17 C.F.R. § 240.10A-3(b)(3). "U.S. listed companies" refers to those companies listed on a U.S. national securities exchange or U.S. automated inter-dealer quotation system (*e.g.,* the NYSE, NASDAQ or AMEX).
3. CNIL is an independent administrative agency in France that regulates French privacy laws.
4. French privacy law requires employers to secure CNIL approval of their privacy policies.
5. Privacy laws are not the only impediment to implementing a SOX whistleblowing procedure in EU countries. For example, a June 15, 2005 labor court ruling in Germany barred Wal-Mart's German subsidiary from implementing major parts of its global code of ethics because of a violation of work council codetermination right.
6. *See* Council Directive 95/46/EC 1995. The EEA countries are the EU member states, plus Iceland, Norway and Liechtenstein.
7. A report that addresses conduct outside the permissible scope of the whistleblowing procedure may be acted upon in very limited circumstances, such as where the company has a legal obligation to act or the action is necessary to prevent a risk to the health or safety of an individual.
8. The four allowable approaches are (i) an intercompany contractual arrangement between the data transferor in the EU and the data recipient outside the EU pursuant to which the recipient is obligated to observe certain data processing principles; (ii) "self-certification" under the Safe Harbor Agreement as negotiated by the United States and the EU (only available for a U.S. data recipient regulated by the Federal Trade Commission or the Department of Transportation); (iii) a binding code of conduct, within the meaning of article 26(2) of the EU Directive; and (iv) transfer of data based on necessity (within the very limited meaning of article 26(1) of the EU Directive) or with the prior consent of the targeted individual. A detailed discussion of these measures is beyond the scope of this client alert. If you require additional information, please do not hesitate to contact any of the attorneys listed at the end of this client alert.
9. The only countries outside the EEA that are deemed to provide adequate protection are Switzerland, Hungary, Canada, Argentina, Guernsey and the Isle of Man.
10. In France, if an employer seeks to terminate an employee through a disciplinary dismissal, the employer must send the employee a letter inviting the employee to a preliminary meeting within two months of becoming aware of an issue potentially giving rise to the dismissal.
11. As explained above, a whistleblowing procedure may allow receipt of reports outside the EEA, subject to certain conditions.
12. On February 1, 2006, the EU Working Party, an independent EU advisory body on data protection and privacy, issued an opinion regarding whistleblowing procedures. The opinion is largely consistent with the Guidance and the Directive, emphasizing that the scope of any such procedure set up in a EU member state generally must be limited to meeting a legal obligation imposed by the member state and anonymous reporting must be discouraged. While a EU Working Party opinion is not a binding law, it has a significant influence on the EU law and policy-making bodies.

Lawyers of Paul Hastings are available to assist with addressing any whistleblowing issues.

London Office
Christopher Walter 44-20-7710-2031
christopherwalter@paulhastings.com

Ray Wann 44-20-7710-2008
raywann@paulhastings.com

Milan Office
Bruno Cova 39-02-30414-000
brunocova@paulhastings.com

Roberto Cornetta 39-02-30414-000
robertocornetta@paulhastings.com

New York Office
Erika Collins 212-318-6789
erikacollins@paulhastings.com

Marjorie Culver 212-318-6650
marjorieculver@paulhastings.com

Kenji Hosokawa 212-318-6874
kenjihosokawa@paulhastings.com

Paris Office
Joel Simon 33-1-42-99-04-45
joelsimon@paulhastings.com

Scott Saks 33-1-42-99-04-57
scottsaks@paulhastings.com

Nicolas Zouaghi-Maulet 33-1-42-99-04-50
nicolaszouaghimaulet@paulhastings.com

David Dumarche 33-1-42-99-04-00
daviddumarche@paulhastings.com