SIDLEY AUSTIN BROWN & WOOD
AND AFFILIATED PARTNERSHIPS

OCTOBER 2005

INFORMATION LAW AND PRIVACY ALERT

The Information Law and Privacy Practice of Sidley Austin Brown & Wood

We offer clients an inter-disciplinary, international group of lawyers focusing on the complex national and international issues of data protection and cyber law. The group includes regulatory compliance lawyers, litigators, financial institution practitioners, health care lawyers, EU specialists, IT licensing and marketing counsel, intellectual property, and white collar lawyers.

Sidley provides services in the following areas:

Privacy and Internet Litigation
Data Breach, Incident Response, and Cybercrime Advice
Global Data Protection and Information Security Programs
International Data Transfer Solutions
Gramm-Leach-Bliley and Financial Privacy
HIPAA and Healthcare Privacy
Workplace Privacy and Employee Monitoring
Outsourcing and Cross-Border Issues
Records Retention and Electronic Discovery
Cyberlaw, E-Commerce, and Internet Issues
Unfair Competition, Consumer Protection, and Marketing
Trademark and Copyright Litigation and Counseling
Website Policies and Domain Name Protection
Trademark and Copyright Litigation and Counseling
Website Policies and Domain Name Protection

For more information, please visit www.sidley.com/cyberlaw, or contact:

Alan Charles Raul
202.736.8477
araul@sidley.com

To receive future copies of the Information Law and Privacy Alert via email, please send your name, company or firm name and email address to Charlotte Green at cgreen@sidley.com

Sarbanes-Oxley meets EU Data Protection

EU data protection laws are being used by data protection authorities to challenge the legitimacy of whistleblower hotlines established in accordance with the US Sarbanes-Oxley Act of 2002 (SOX). Recent decisions in France and Germany have resulted in US-listed companies having to balance obligations under SOX with potentially inconsistent local EU data protection laws in relation to whistleblowing. French officials met on September 12 with the U.S. Securities and Exchange Commission to try to work out a solution. However, on September 15 a French court ordered a local subsidiary of an American firm to terminate a whistleblower hotline and pay approximately $1500 in damages to an employee works council and a labor union. As a result of these decisions, some companies in Europe may be suspending their hotlines or modifying their whistleblower policies. This issue is not restricted to just France and Germany as other data protection authorities throughout the EU are considering whether whistleblowing hotlines may be contrary to their local data protection laws.

Sarbanes-Oxley Act

SOX requires US-listed companies and their affiliates worldwide to make confidential anonymous whistleblower channels available to their employees. Such companies have sought to fulfill their SOX obligations by introducing measures such as telephone hotlines, websites and e-mail addresses to which employees may submit their concerns anonymously. SOX §301(4) provides that a company's audit committee shall establish procedures for the receipt, retention, and treatment of complaints received by the company regarding accounting, internal accounting controls, or auditing matters and the confidential, anonymous submission by employees of the company of concerns regarding questionable accounting or auditing matters.

US-based companies have introduced the same channels of reporting for their European group companies so that overseas employees have facilities through which they may bring their concerns to the attention of the US company's relevant personnel. In addition, many companies employ specialist third parties to operate whistleblower hotlines and other channels.

Conflicts with EU Data Protection

In France, two companies approached the French Data Protection Authority (CNIL) to register their anonymous whistleblower facilities for use in France. One company proposed the use of a US fax number and postal address for employees to

report concerns. The other company sought to register a group telephone hotline and e-mail address for its employees.

In response, CNIL decided that neither company's proposals were satisfactory for the following data protection and privacy reasons:[1]

- individuals who were the subject of statements made by whistleblowers may not be able to access or respond to the allegations made against them;
- employees against whom allegations were made may not have the means to defend themselves or oppose subsequent criminal or civil proceedings; and
- the whistleblower tools were disproportionate to the aims they sought to achieve. Other anti-fraud mechanisms such as employee training, alerts and audits by accountants and the use of the courts to enforce labour laws would be less privacy-invasive and less prone to abuse than whistleblower procedures.

CNIL also stated that, as a matter of principle, whistleblower practices were unacceptable in France because they increased the risk of a person anonymously denouncing another.

CNIL's decisions have left US-listed companies in a state of uncertainty as to how to comply with the requirements under SOX and data protection law requirements in France and potentially other EU Member States. Currently, there are on-going discussions between CNIL and the SEC to try to find a way through the conflicting requirements. Guidance is expected from CNIL by the end of November 2005. In the interim, some companies in France have ceased using whistleblower hotlines until a resolution has been found. Other companies are seeking to maintain their whistleblower hotlines while considering their existing policies and procedures to see if amendments can be made.

Even more recently, on September 15, the French Tribunal de Grande Instance de Libourne awarded an employee works council and labor union about $1500 in damages and ordered that the "ethics hotline" established by BSN-Glasspack, a local subsidiary of Owens-Illinois, was disproportionate to the potential wrongdoing that would be disclosed as a result of the whistleblower hotline. The French court accepted the plaintiffs' arguments that the hotline could violate workplace privacy rights and the right to defend against allegations of wrongdoing. This ruling in *CE BSN-Glasspack* v. *BSN-Glasspack* is, of course, consistent with the CNIL's position.

Doubts as to the legality of whistleblower mechanisms have also been expressed in several other EU Member States including Belgium, Denmark, Germany, Greece, Italy, Luxembourg, Portugal and Spain. For example, a whistleblower hotline and sections of an international group's code of conduct were recently struck down by the German court[2] because of infringements of labour law. While in Belgium, the Belgian Data Protection Authority, the Commission for the Protection of Privacy (the Commission), may be preparing to take a similar course of action to that taken by CNIL in France. Belgian listed companies are required to comply with the Lippens Code (the Belgian Code on Corporate Governance), and certain companies have established whistleblower hotlines in an attempt to satisfy the Code. The use of a whistleblower hotline by at least one bank is currently under investigation by the Commission for non-compliance with data protection laws and there are serious concerns as to whether similar

[1] Decision 2005-110 rendered on 26 May 2005 and Decision 2005-111 rendered on 26 May 2005.

[2] Arbeitsgericht Wuppertal, Court Order dated 15 June, 2005, 5 BV 20/05.

whistleblower hotlines established pursuant to SOX or the Code will satisfy Belgian data protection laws.

A different position on whistleblowers is presented in the UK, where it is thought that the appropriate use of whistleblower facilities would not, in principle, raise concerns as the UK has legislation[3] specifically dealing with whistleblowers.

Practical Steps

In evaluating their potential liability under EU data protection laws, US-listed companies should ascertain the application of local EU data protection laws in those Member States in which they operate. Companies should closely follow developments concerning whistleblowing in each of these EU Member States and consider any guidance on this issue produced by the local data protection authority. Companies should also consider the following practical measures to reduce the likelihood of breaching local data protection laws:

- consulting with local data protection authorities and works councils before implementing whistleblower practices;
- ensuring that employees' due process rights are preserved;
- ensuring that regulatory compliance programs, where possible, include methods beyond whistleblowers, such as employee training and audits;
- ensuring that whistleblower allegation data is retained for only as long as necessary and that such data is kept separate from an individual's personnel file (unless the investigation reveals wrongdoing); and
- ensuring that adequate data protection steps have been taken where data is to be transferred outside of the EU by using appropriate EU model data transfer agreements or transferring to entities in the US that are members of the Safe Harbour Scheme.

***

Sidley's Information Law and Privacy Practice group regularly publishes articles on topics related to its practice on the firm's CyberLaw website at http://www.sidley.com/cyberlaw.

More Information about the subject of this Alert may be obtained from:

John M. Casanova
Tel: +44 (0) 20 7360 3739
jcasanova@sidley.com

William R.M. Long
Tel: +44 (0) 20 7360 2061
wlong@sidley.com

Alan Charles Raul
Tel: (202) 736 8477
araul@sidley.com

Edward R. McNicholas
Tel: (202) 736 8010
emcnicholas@sidley.com

[3] Public Interest Disclosure Act 1998.