

World Data Protection Report

International Information for International Businesses

Monthly news and analysis of data protection and privacy issues from around the world

Anonymous Sarbanes-Oxley Hotlines in the E.U.: Practical Compliance Guidance for Global Companies

*Mark E. Schreiber, Jeffrey M. Held, Palmer & Dodge LLP, Boston, MA
Robert T.J. Bond, Faegre & Benson LLP, London
Christian Runte, CMS Hasche Sigle, Munich
Raphaël Dana, Soulier Avocats, Paris
Kate Flower, Eversheds LLP, Birmingham*

Reprinted from the August 2005 issue of BNA International's
World Data Protection Report



www.bnai.com

Legislation and Guidance

Anonymous Sarbanes-Oxley Hotlines in the E.U.: Practical Compliance Guidance for Global Companies

By Mark E. Schreiber, Jeffrey M. Held, Palmer & Dodge LLP, Boston, MA; Robert T.J. Bond, Faegre & Benson LLP, London; Christian Runte, CMS Hasche Sigle, Munich; Raphaël Dana, Soulier Avocats, Paris; and Kate Flower, Eversheds LLP, Birmingham. The firms of all the contributing authors are members of the World Law Group, www.theworldlawgroup.com

The recent decisions in France¹ and Germany² that anonymous employee whistle-blowing hotlines, without certain precautions, are invalid or unlawful in those countries is causing concern for many multinational public companies that must comply with the U.S. Sarbanes-Oxley Act of 2002 ("SOX") and related U.S. rules.³ SOX requires an anonymous method for employees to report concerns related to accounting and financial matters⁴ and the adoption of a code of ethical conduct designed to promote prompt reporting of code violations.⁵

The French CNIL decisions and German Labor Court case reflect the historical unease in many E.U. countries over the concept of encouraging individuals to inform against others anonymously and without an immediate opportunity for the accused person to respond. Many U.S. companies maintain subsidiaries and employees in the European Union where the anonymous hotlines and other reporting mechanisms are now in place; those same companies must now consider data protection, labor and human rights legislation in the European Union, as well as the underlying historical stigma attached to the interpretation of a whistleblower as an informer. In several E.U. Member States, the U.S. SOX requirements may be in direct conflict with recent decisions on the interpretation of such E.U. legislation.

Depending on further developments in these jurisdictions and interpretations by appropriate bodies, resolution of the apparent conflicts may require special relief from U.S. regulators, such as the SEC, and/or the CNIL or other E.U. data protection authorities. Pending regulators' further interpretation or guidance, what should U.S. multinationals do? This article offers interim guidance on steps companies may wish to consider to minimize the risks in E.U. countries while still complying with SOX.

U.S. Requirements

Control Systems

Maintaining effective global control systems is important to companies subject to U.S. law to ensure that possible code of ethics violations, misconduct and fraud are reported promptly. SOX demands that companies have control systems in place to ensure they can make timely and truthful public disclosures

as required by applicable securities laws and issue accurate financial statements.⁶ This in turn necessitates adequate reporting or, in U.S. parlance, "whistleblowing" procedures, in order to detect fraud, permit proper information flow and identify issues that could impact the veracity of the financial statements. A company's independent auditors will audit these controls and publicly disclose the results of that audit. Accordingly, maintenance of a proper "tone at the top" and a "culture of compliance" (buzz-words in the United States) has become a hallmark of appropriate corporate governance. The absence of a proper control environment can cause a company to fail an evaluation of its controls.

Accounting-Related Complaint Procedures

In addition, SOX and the related U.S. Securities and Exchange Commission ("SEC") and stock exchange regulations require audit committees of companies listed on a stock exchange to establish procedures for the:

- confidential, anonymous submission by employees of that company of concerns regarding questionable accounting or auditing; and
- receipt, retention and treatment of complaints received by that company relating to accounting, internal accounting controls or auditing matters.⁷

No particular complaint submission method is prescribed; companies can, therefore, provide for a variety of employee reporting methods, such as phone, e-mail, mail, fax, and/or a complaint drop-box, *provided that at least one confidential, anonymous method is available to employees*. The U.S. Congress intended to provide an environment where fraud and accounting impropriety would be discouraged and whistleblowers encouraged to come forward. In the wake of scandals at companies like Enron and Worldcom, the U.S. authorities sought to restore confidence in the financial statements of U.S. public companies and the U.S. markets generally.

Companies subject to SOX that fail to meet these requirements may potentially face SEC enforcement action, potential SEC civil penalties and/or de-listing from the stock exchange on which their securities are traded. Because of the severe consequences of SOX violations, U.S. companies will likely decide to adhere to minimum SOX requirements, unless the SEC somehow relieves them of that burden, even at the risk of potential E.U. infractions.

Hotlines and Anonymity

Many companies outsource the reporting function to a third-party service provider using a confidential hotline, web service or other vehicle so that individuals can register

complaints. An array of potential complaint categories is common, and a mechanism is created for complaints to be routed to the appropriate person/department. For example, information concerning accounting or the financial statements would generally end up delivered to the audit committee, the chairman of which is usually a person resident in the U.S. Matters that are labor-related, such as allegations of sexual harassment, might be sent to the local director of human resources or regional vice president.

The U.S. purpose of the confidential and anonymous requirement is to encourage employees to come forward without fear of reprisal. This mechanism was meant to assist bringing the information to the right levels within the company, including, if required, the board of directors. Accordingly, employees who “blow the whistle” on financial improprieties under the provisions of SOX not only have protection from retaliation but also have a complaint mechanism through the U.S. Dept. of Labor,⁸ and a later right to file suit.

Code of Conduct

The SEC also requires that public companies disclose in their proxy statements whether or not they have adopted a code of ethics for certain of their senior executives that meets certain minimum requirements. The U.S. stock exchanges have affirmative requirements to maintain such a code of ethics (which they have expanded to apply to all employees, directors and officers), and require that the code have an enforcement mechanism. A code of ethics must be reasonably designed to promote ethical conduct and handling of conflicts of interest, timely and accurate public disclosures and compliance with laws. In addition, the code must promote prompt internal reporting of, and contain an enforcement mechanism for, code violations.⁹

Codes of conduct are typically broad and allow employees or others to make complaints about topics such as fraud, financial matters, conflicts of interest, employment, environmental and other matters using the same hotline or other reporting mechanisms implemented for accounting-related complaints. Complaints concerning employees that involve both financial statement and related employment issues further complicate matters. Nevertheless, many U.S. companies view it as advisable to permit numerous matters to be included in the code and reporting mechanism, regardless of whether the subject matter is related to accounting or financial fraud issues.

E.U. Overview

Rulings by the French data protection agency (CNIL) against McDonald’s and CEAC/Exide Technologies and the German Labor Court ruling against Wal-Mart now prevent these companies from implementing hotlines in those countries, at least without further changes or activities.

The German decision ruled that the Wal-Mart hotline was illegal because it had been implemented by Wal-Mart without addressing the Section 87 Right of Co-Determination under the German Works Council Constitution Act.¹⁰ In other words, Wal-Mart might have been able to implement a satisfactory hotline if it had first consulted with the works council, which has a right of co-determination in “matters relating to the rules of operation of the establishment and conduct of employees”.

The decision in France in the McDonald’s case was not based on labor law but rather on the fundamental principles of individual rights to privacy, human rights, human dignity and aspects of data protection. Specific mention was made in the CNIL decision that the,

“[making of] an ethics alert in an anonymous manner could only reinforce the risk of *slandorous denunciations*. Moreover, the commission considers that the system was disproportionate to the objectives sought and the risks of slanderous denunciations and the stigmatization of employees who are the subject of an ‘ethics alert’ ”.

In addition, a Report by Public Concerns at Work, a U.K. not for profit organisation on behalf of the European Commission, states that,

“the commission consider[ed], finally, that the employee [that] is subject to [the hotline] alert would not be, by definition, informed as soon as the data questioning their professional or personal integrity is recorded, and as such they would not have the means to contest the processing of such data”.¹¹

Although not an issue for the McDonald’s and Wal-Mart’s decisions, the implementation of whistleblowing hotlines in the European Union not only raises issues of anonymity but also the regulatory infrastructure within which such hotlines are implemented. E.U. Data Protection laws¹² require, among other things, that in relation to personal data:

- an individual has a right to know what data is being processed about them;
- personal data has to be processed fairly and lawfully;
- personal data must be kept for no longer than is necessary and must be accurate and up-to-date;
- personal data must be, at all times, kept secure and where processed by a third party be managed securely; and
- personal data should not be transferred outside the European Economic Area to any other country that does not have adequate protection for the rights of the individual.

In many of the current implementations of whistleblowing hotlines, compliance with the above fundamental E.U. data protection rights may not have been adequately addressed or may not have been addressed at all. For example, E.U. individuals need to be notified what data will or may be collected about them. Without a detailed statement and policy concerning whistleblowing, this principle may be violated.

General Risk Mitigation Techniques

There appears to be no single solution that would currently provide a U.S. publicly-traded multi-national company with the ability to comply fully with SOX as well as the data protection and labor laws of all E.U. Member States. Possible near term options, either individually or taken together, that are responsive to concerns of French, German or other E.U. Member States’ data protection or labor authorities include the following:

- (1) Prompt notification to the person accused or reported on of the details of the accusation, and right to respond/contest or rectify information.

Prompt notice or disclosure of complaint details to the accused or reported-on individual may be the most important factor in having U.S.-styled hotlines approved by E.U. data protection authorities, at least in France, if not elsewhere. A choice modality for the employer to elect such disclosures would not violate or impact SOX laws unless notification to the accused individual materially compromises the company's control environment. As a matter of investigatory best practices, it may be viewed by some as imprudent to disclose to the accused person the full details of the complaint before certain parts of an investigation are complete, particularly in fraud matters. This is, however, a strategic choice and data protection laws in many, if not all E.U. countries will require such disclosures.

(2) Keeping the personal data of the person accused or reported on in the E.U. country and not transmitting it to the U.S.

As to labor, employment, extraneous or non-SOX issues or matters not material to financial statements, this may well work. As respects any reports that involve financial statements, fraud, auditing or any material matter, this may not be a practical option for companies whose nerve centre is in the United States; these reports will need to be forwarded immediately, and (as to financial matters) generally sent to the chairman of the audit committee in the United States. SOX rules require U.S. audit committees to receive, handle and treat complaints within their subject matter area. U.S. publicly traded companies need to maintain a system of controls which permit rapid analysis, investigation and remedial action as to events or occurrences that are potentially discloseable and/or which could materially impact their financial statements.

If personal data is transmitted from the E.U. branch office or an employee reporting from the European Union, the U.S. entity recipient should have in place an appropriate cross-border transfer solution: either consent of the individual reporting, a data protection agreement (either data processor or data controller) or have certified for the U.S. Safe Harbor.

(3) Conducting investigations resulting from SOX reporting in the local E.U. country only.

This may be possible for routine employment or related matters not within the purview of the audit committee, such as labor or employment issues that do not implicate financial statements or accounting. The difficulty with this option is that many matters that could have a potential impact on accounting or financial statements also involve individual behaviour. The same issues as in (2), above, also apply.

(4) Limiting or adjusting hotline or reporting mechanism (and perhaps scope of the company code of conduct in that country) to required SOX provisions like audit or financial irregularity issues and not labor or employment ones.

Titration or limiting hotline, web or other reporting modalities to narrow SOX-required subjects, like fraud and financial matters, would help satisfy E.U. country data protection authorities and perhaps even E.U. country labor officials. This option could potentially be implemented without infringing on SOX obligations, especially as to broad codes that encompass many areas not required by SOX. Code of ethics and conduct must include provisions that require prompt reporting of code violations, the subject of which needs to include ethical conduct, conflicts of interest, SEC disclosure matters, violations of law and other improprieties that in some cases impact

financial statements and accounting. As long as these are adhered to, SOX is satisfied. This approach, nevertheless, may be viewed as impractical from an overall compliance perspective by some companies.

(5) Asking reporting individual to allow his/her name to be used in report, and/or having hotline reporting individual asked not to identify "accused" individual by name unless necessary.

This would avoid some anonymous reporting and appears to be acceptable within the SOX framework, as long as at least one anonymous reporting mechanism was made available. Voluntary disclosure by the reporting individual of his/her name would not violate SOX. If the reporting individual insists on anonymity, this must be respected under SOX, and the anonymity itself seems to run afoul of E.U. data protection principles and in particular, the recent French decisions. In some circumstances, depending on the nature of the allegations, it may be impractical to report wrongdoing without disclosing the accused's name in order to give the company a meaningful opportunity to investigate.

(6) Limiting or exempting E.U.-based employees from the duty to report.

This would help satisfy labor courts in Germany and perhaps elsewhere. Many SOX-inspired codes of conduct require employees to report violations and risk discipline if they do not report clear or known violations. It is not clear how U.S. companies will react to this suggestion as it presents a lesser level of reporting obligations for E.U. versus U.S. employees on critical topics. See issues in (4), above.

(7) Negotiate with the Works Council if the employer has one.

If subject to an E.U. Works Council requirement, the employer could voluntarily try to negotiate mutually acceptable hotline, reporting and code of conduct terms encompassing items (1) to (6), above. Success in this regard would also help with local data protection authority issues. A reduced version only addressing minimum SOX standards may not be acceptable to some U.S. companies.

(8) Plan strategy based on the E.U. countries in which the entity operates.

Britain and Ireland appear more receptive to hotlines and reporting than France, Germany and Belgium and probably Spain, Portugal, Italy and others. Where the company operates in the European Union may determine its risk profile.

Individual E.U. Member State Analysis/Solutions

Germany

From a German legal perspective, the implementation of a whistleblower hotline and binding codes of ethics and conduct involves both privacy and labor law issues. The recent decision of the Labor Law Court of Wuppertal¹³ focuses almost entirely on the labor law aspects and leaves aside possible data protection issues. However, both aspects have to be taken into account when implementing code of conducts and whistleblower hotlines in Germany.

Wal-Mart Decision

In its Wal-Mart decision the Labor Law Court of Wuppertal held that major parts of Wal-Mart's code of conduct were

invalid and that Wal-Mart had to stop providing its whistleblower hotline for German Wal-Mart employees until an agreement with the works council of Wal-Mart is reached. According to the decision¹⁴ Wal-Mart tried to implement a German language version of its global code of conduct and obligated the employees of the German subsidiaries to adhere to its provisions. The code of conduct in particular contained guidelines on the prevention and handling of conflict of interests, confidentiality, fair conduct of daily business and the protection of company assets. All employees were obligated to report any possible violations of the code to the company. In order to do so, Wal-Mart offered a toll-free telephone hotline which would treat information provided by whistleblowers on an anonymous basis.

The works council of the German subsidiary of Wal-Mart was not involved in the drafting and implementing of the code of conduct. The works council subsequently took the German subsidiary of Wal-Mart to court and argued that the implementation of the code of conduct in Germany would be subject to a co-determination right according to the German Works Council Constitution Act. Wal-Mart's works council asked the court to establish that:

- the implementation of the code of conduct as a whole;
- alternatively, the individual guidelines of the code of conduct; and
- the operation of the telephone hotline would be subject to a co-determination right and therefore would require the consent of the Wal-Mart works council.

The Labor Law Court of Wuppertal held that the implementation of a code of conduct as a whole does not require the consent of the works council *per se*. In fact, the Court stated that some of the provisions of the code can be implemented without the consent of the works council, including those pertaining to financial integrity and accounting, insider trading, confidentiality and trade secrets, supplier/customer relationships, anti-discrimination and the use of company property. However, the implementation and operation of the telephone hotline and provisions relating to presents and gifts, media statements, harassment, inappropriate behaviour, private relationships, access to employee files, and alcohol and drug abuse, would be subject to the consent of the works council. In addition, some of these provisions, such as those relating to "personality rights" (*i.e.*, private relations with co-workers, private life issues and the like), would likely be unenforceable even if approved by the works council under existing German law. Although the decision is not yet legally final, we assume that the decision will be upheld if appealed (although such an appeal could take six months or longer to resolve). This does not mean however, that a whistleblower hotline or the implementation of a code of conduct and ethics would not be feasible in Germany. To do so, it is necessary, however, to give some additional consideration to German data protection issues and labor law.

The Works Council and the Right of Co-Determination

The Wal-Mart decision is based on a particularity of German labor law, namely the right of co-determination which is contained in the Works Council Constitution Act. The Act stipulates that works councils must be established in all companies that have five or more regular employees. The function of the works council is to protect the "collective labor rights" of the employees of the company. In the Works Council

Constitution Act, works councils in Germany are given extensive rights of information, consultation and co-determination. In particular, the works council is granted an explicit set of co-determination rights on matters where the work council has actual joint decision-making authority. These rights are only granted if the employees choose to actually elect a works council.

Examples of those areas in which a works council has joint decision-making authority with management are not only the regulation of overtime and reduced working hours but also the introduction and operation of technical devices to monitor the behaviour or performance of the employees (section 87 No. 6 German Works Council Constitution Act), and matters relating to the rules of operation of the establishment and the conduct of employees in the establishment (section 87 No. 1 German Works Council Constitution Act). In the Wal-Mart decision the court held that the introduction of binding rules and a hotline, where the employees were obligated to adhere to rules which had no direct connection to the performance of the contractual obligation of the employee were subject to co-determination rights of both section 87 No. 1 and No. 6 German Works Council Constitution Act. Failure to obtain the consent of the works council would render the introduction of these parts of the code of conduct – including the whistleblower hotline – impermissible.

The usual way to obtain the consent of the works council is for the works council and the management to agree upon a works agreement (*Betriebsvereinbarung*). Failure to reach an agreement leads to a decision of an arbitration board. Without agreement with the works council or a decision of the arbitration board, the introduction of binding codes of conduct is not possible. Generally, work councils understand the necessity of complying with SOX and are willing to agree to the implementation of codes of conduct. Irrespective of such codes, to report fraud and corruption within the company has always been accepted as being part of the employees' contractual obligation to the employer. However, in German employment law the extent to which the employer may require binding rules regarding personal conduct, including outside of the working environment, is narrow. Any negotiation with a works council therefore may result in the limitation of a code of conduct.

Data Protection Laws

From a data protection perspective, German data protection law – unlike in France – does not require a company to register an anonymous telephone hotline with the data protection authorities or to apply for permission. However, the operation of a SOX whistleblower telephone hotline comes with the same privacy and regulatory problems that have to be dealt with in the operation of every call centre. In most cases companies use software-based ticketing systems where personal data regarding the alleged wrongdoer and possibly the caller himself is collected, processed and ultimately transferred to the U.S. parent company. All of these actions need to be in compliance with European and German data protection legislation.

Additional problems arise where the operation of the system is outsourced to a third party. German data protection law does not recognise an intra-group privilege for the transfer of data. Any transfer of personal data to another company – either part of the same group or random third party provider – requires

sufficient legal permission or the consent of the individual concerned. In order to avoid these additional requirements an external provider would have to act as data processing agent. This requires agreement on a written contract which contains explicit provisions on the handling and processing of the personal data along with measures to ensure that the company itself remains in control of the processing and collection of data. Where the data is ultimately transferred to the United States, either the EC Commission standard contractual clauses have to be implemented or the U.S. company has to certify according to the Safe Harbor regulations.

Conclusions for Germany

The introduction of a whistleblower hotline in German subsidiaries involves certain obstacles. These, however, can be overcome. Where a works council is in place, the introduction of a SOX-compliant code of conduct and whistleblower system will usually be subject to negotiations with the works council and respective works agreements. Because the code provisions the court in the Wal-Mart decision deemed subject to the right of co-determination are limited, it is likely agreement with the works council could be reached. Other sections of an ethics code – in particular regarding personal relationships – might be incompatible with German labor law and therefore unenforceable in Germany, irrespective of any agreement with the works council. These narrow provisions could be omitted from a code of ethics intending to comply with SOX. In any case the implementation of a whistleblower system, either by a telephone hotline or other electronic means (e.g., e-mail) requires special attention to German data protection laws.

France

In the two decisions issued in May 2005,¹⁵ the CNIL (Commission Nationale de l'Informatique et des Libertés, i.e., French National Commission for Data Protection and the Liberties, or French Data Protection Authority), rejected the proposed use of U.S.-style whistleblowing hotlines in France on the grounds of data protection. This has an important impact for the French subsidiaries of U.S. public companies which must comply with the SOX provisions.

Summary of Recent CNIL Decisions

In order to comply with the SOX requirements, both companies (McDonald's and CEAC/Exide Technologies) sought permission to establish anonymous employee "whistleblower" hotlines and had contacted the CNIL to register the systems for use in France. These hotlines would allow employees to "blow the whistle" on perceived wrongdoings by colleagues using telephone, fax, post or e-mail. McDonald's had crafted a detailed and thoughtful implementation protocol, including a data transfer agreement, for CNIL approval. Although both companies had apparently complied with the 1978 French Data Protection Act as modified in 2004, the CNIL decided that these hotlines would be illegal for the following reasons:

- *Lack of transparency:* individuals who are the object of a whistleblower's allegations may not be able to access or reply to the accusations made against them. This could result in disciplinary action or even dismissal for the individual.

- *Unfairness:* employees so accused would not have the means to defend themselves or oppose the proceedings which may involve criminal charges.
- *Professional ethics:* this tool is disproportionate to the aim it seeks to achieve.

More generally, the CNIL expressed serious reservations about whistleblowing in its current form as it is contrary to French historical and social principles regarding slanderous denunciation from an anonymous accuser.

For the present, these two decisions apparently mean that French law is in direct conflict with SOX. The CNIL is aware of this and has asked the French Employment Minister and the competent authorities in the United States to resolve this issue. The French decisions have only recently been published and there is no expert government commentary on how to deal with this problem. It is therefore unclear which of the several factors cited by the CNIL would be determinative. It is likely, however, that the anonymous feature and the failure to immediately inform the accused, thus not permitting him/her to respond quickly are the elements deemed most offensive.

Data Protection Laws

In accordance with the French data protection law,¹⁶ data has to be collected and handled fairly and lawfully. Data collected have to be adequate, pertinent and not excessive with regards to the means for which they are collected and later processed. Moreover, appropriate measures have to be taken to ensure that inaccurate or incomplete data are deleted or rectified. The individual concerned has to be able to access and correct such collected data.

Data collection, sharing and disclosure, can be implemented within a company's code of conduct, but whistleblowing hotlines must comply with the principles enacted by French law and European texts, especially the Convention for the Protection of Individuals with regards to Automated Management of Personal Data (Convention 108 of the European Council, dated January 28, 1981) as well as Directive 95/46/EC of October 24, 1995.

French law requires employees to alert the authorities when they suspect that financial improprieties have taken place but French labor law does not protect the job security of an employee because the whistleblower's dismissal may be justified under the principles of "obligations to respect confidentiality", "link of subordination", and "abuse of freedom on expression". Employees do in fact have the right to make disclosures of breaches of law provided that such disclosures are not false, are communicated in good faith, and without the direct intention to cause prejudice to the employer. The French Supreme Court in a relatively recent decision¹⁷ ruled that where an employee disclosed to a Labor Inspector facts concerning financial impropriety by an employer, this did not constitute misconduct *per se*. Under French law there is a difference between the duty of an employee in good faith to disclose improprieties as opposed to what the CNIL deemed to be the possibility under the McDonald's hotline of making "slanderous denunciations."

Historical Context

Would anonymous hotlines protect a French employee who blew the whistle under any circumstances? Anonymity, for historical

and cultural reasons, makes the reporting person an “informer” in the eyes of the French Courts and citizens.

The implementation of a French based ethics committee (which could be a “branch” of the Workers’ Council) that would manage whistleblowing calls is a solution that has been adopted by some multi-nationals, including Shell. In such instances the whistleblowers have to identify themselves, but the committee commits itself to keeping the whistleblower’s identity secret. The problem remains however as to how to determine the scope and parameter of such confidentiality obligations. One method for securing whistleblower protection is to pass legislation prohibiting retaliation as has occurred in the United Kingdom.¹⁸

United Kingdom

The French and German rulings are likely to also be of concern to U.K. employers, since anonymous hotlines are commonly used to facilitate compliance with U.K. whistleblowing laws. Under the U.K. Public Interest Disclosure Act,¹⁹ any employee who is dismissed or subject to a detriment on grounds of “blowing the whistle” can be awarded unlimited compensation. U.K. employers now face the difficult task of balancing the rights of employees blowing the whistle against the legitimate interests of employees facing disciplinary action. Employees dismissed as a consequence of an anonymous report have little to lose in bringing a subject access request or complaint under the U.K. Data Protection Act (“the Act”) and U.K. employers need to make sure they consider the implications of these rights. That said, SOX hotlines and codes of ethics should not generally violate existing law in the United Kingdom.

Rights of Subject Access

An individual is entitled to apply to any organisation holding personal information about him/her and, subject to certain exemptions, to request a copy of that data. Some information gathered through whistleblowing hotlines may be exempt from disclosure if it falls within one of the subject access exemptions, the most likely being:

- if it contains third party personal data (most likely, the identifying details of the informant) which cannot be effectively made anonymous and, taking into account all relevant factors, the third party’s interests in having his or her details kept confidential outweigh the applicant’s rights to see a copy of the data;
- if the information is subject to legal privilege;
- if the data contains a record of the employer’s intentions in negotiations, and disclosure of that information would prejudice the employer’s position in relation to such negotiations, or
- following the recent case of *Durant v. Financial Services Authority*,²⁰ to the extent the data is held in unstructured paper files (as opposed to electronically) and not categorised by reference to the individual or any other personal identifiers.

Complaints

An aggrieved individual can make a complaint to the U.K. Office of the Information Commissioner. The individual will be entitled to compensation if he or she can demonstrate that he or she has suffered damage and distress as a result of the breach. The biggest risk to organisations, however, is the effect on their

reputation – all complaints are published and competitors are often only too happy to point the finger.

Minimising the Risk

Employers need to make sure that their use of any whistleblowing hotline complies with the eight key principles of the Act (as mentioned above), the most important being:

- *Fair processing*: employers must ensure that they have a clear, comprehensive policy in place, setting out full details of the whistleblowing process, what information will be collected and retained, how it will be used, who will have access to such information and any other relevant information (for example, whether the information will be transferred outside the EEA or to another group company or authority). Employers must ensure that all employees are made aware of the policy at regular intervals.
- *Proportionality*: employers should have clear procedures in place to ensure that they only retain information which is *necessary* for the purposes of investigating the issues raised and that any ancillary information is promptly deleted. Only staff who have a need to access whistleblowing information for the purposes of carrying out investigations should be able to do so.
- *Retention of data*: employers should consider how long they *really* need to keep details of a complaint once investigations have been concluded or the matter has been otherwise resolved. As far as possible, such details should be made anonymous and kept in summary format only.
- *Accuracy*: employers should ensure that they are only using information gathered through whistleblowing complaints as a basis for further investigation, rather than as grounds for disciplinary action in isolation. The accused party should be informed of the complaint as soon as possible and given a reasonable opportunity to respond. Any information which is investigated and established as inaccurate must be deleted.
- *Security*: employers should review their security procedures to ensure that they are happy that the steps they are taking are proportionate to the likely consequences of unauthorised access, loss or destruction of personal data.

As SOX requires employees to be offered anonymity as an option, this is unlikely to be questioned under U.K. data protection laws. However, employers could consider inviting informants to waive any rights to anonymity as this would make the process easier to administer. If the informer chooses to waive their right to remain anonymous, the employer knows that it can disclose information to the other party without fear of breaching the Act. Similarly, if the informant refuses consent, then this would be a major factor against disclosing anything which would identify the informant. Employers must bear in mind that, for such consent to be valid, it must have been given freely, in full knowledge of the process and without any fear of adverse consequences of withholding consent.

As much as possible, employers should try to deal with whistleblowing disclosures in the country in which they were made (or at least within the EEA) to avoid having to put in place data transfer agreements (or equivalent protections) with companies to which the information is transferred.

Before putting in place or continuing a whistleblowing hotline, employers should carry out a risk assessment, highlighting the specific issues they are looking to address, how they have considered the data protection implications set out in this article and how they have arrived at the conclusion that implementing a hotline is proportionate to the risk identified.

Finally, organisations need to remember that they remain primarily liable for any breaches of the Act which may be committed by their third party agents. They need to ensure that they have agreements in place with such agents which provide, as a minimum, that the agent will act only on the instructions of the company when processing personal information and will have appropriate security measures in place to protect the data. If the hotline is located outside the European Economic Area²¹ or any of the territories considered by the European Commission to have adequate data protection laws in place,²² agents should either be signed up to a “data transfer” agreement in the form approved by the European Commission or, if based in the United States, certify under the Safe Harbor regime implemented by the U.S. Department of Commerce.

Conclusions for U.K.

Early indications from the U.K. Information Commissioners Office (ICO) are that it will not be following the French and German approach. The ICO’s view is that the appropriate use of such helplines by organisations would not, in principle, raise concerns. However, where organisations misuse hotlines for inappropriate information gathering purposes (for example, recording details of out-of-office activities), there may be data protection implications. To date, the Information Commissioner has not received any complaints from individuals affected by anonymous hotline reporting. For now, then, hotlines should not fall foul of the U.K. Data Protection Act provided that employers use the hotlines with care and follow the Act’s key principles. Accordingly, information gathered must be proportionate to the purpose(s) for which it needs to be used and any superfluous information must be deleted. Overall, data should not be kept for longer than objectively necessary or as otherwise required by legislation. Subject to any anonymity requirements, employees against whom complaints are made must be given the opportunity to respond to allegations and employers must ensure that data gathered through such hotlines is used as a basis for further investigation only.

Conclusion

The options outlined earlier should reduce the company’s risk profile while complying with SOX. There remains a significant difficulty for E.U. subsidiaries of American headquartered companies adopting “one size fits all” hotline and code of conduct policies. Even if hotline policies were drafted and implemented in accordance with E.U. data protection and labor laws, it seems that the issues of anonymity and the accused’s right to respond would, at least in France, still provide a legal barrier and a fundamental problem. There is no easy or quick solution and an updated country-by-country analysis will be required. Ultimately, the SEC may weigh in or intervene, but in the meantime, the steps outlined above should be considered and tailored to the company’s risk tolerance.

1 Decision 2005-110 of May 26, 2005 (Group McDonald’s France) and CNIL Decision 2005-111 of May 26, 2005 (Exide Technologies). <English translation>. The English translations available at: www.theworldlawgroup.com/newsletter/details.asp?ID=12463671

22005 and www.theworldlawgroup.com/newsletter/details.asp?ID=12434871 22005.

2 The 5th Division of the Wuppertal Labour Court on June 15, 2005. Arbeitsgericht Wuppertal, Court Order dated June 15, 2005, 5 BV 20/05; English translation available at www.theworldlawgroup.com/newsletter/details.asp?ID=74555728 2005.

3 Public Company Accounting and Investor Protection Act 2002.

4 Section 301 of the Sarbanes-Oxley Act of 2002; SEC Rule 10A-3(b)(3) promulgated under the Securities Exchange Act of 1934; NASDAQ Rule 4350(d)(3); and NYSE Listed Company Manual Section 303A(6).

5 Section 406 of the Sarbanes-Oxley Act of 2002; SEC Item 406 of Regulation S-K; NASDAQ Rule 4350(n) and NYSE Listed Company Manual Section 303A(10).

6 Section 404 of the Sarbanes-Oxley Act of 2002; SEC Rules 13a-15 and 15d-15 promulgated under the Securities Act of 1934.

7 Section 301 of the Sarbanes-Oxley Act of 2002; SEC Rule 10A-3(b)(3) promulgated under the Securities Exchange Act of 1934; NASDAQ Rule 4350(d)(3); and NYSE Listed Company Manual Section 303A(6).

8 Section 806 of the Sarbanes-Oxley Act of 2002.

9 Section 406 of the Sarbanes-Oxley Act of 2002; SEC Item 406 of Regulation S-K; NASDAQ Rule 4350(n) and NYSE Listed Company Manual Section 303A(10).

10 German Works Council Constitution Act (Betriebsverfassungsgesetz – BetrVG).

11 Whistleblowing, Fraud & The European Union – ISBN 1 898809 20 8.

12 (95/46/EC).

13 Arbeitsgericht Wuppertal, Court Order dated June 15, 2005, 5 BV 20/05; English translation available at www.theworldlawgroup.com/newsletter/details.asp?ID=74555728 2005.

14 Arbeitsgericht Wuppertal, Court Order dated June 15, 2005, 5 BV 20/05.

15 The English translations of the decisions available at: www.theworldlawgroup.com/newsletter/details.asp?ID=12463671 22005 and www.theworldlawgroup.com/newsletter/details.asp?ID=12434871 22005.

16 Articles 6 and 7 of Law n° 78-17 dated January 6, 1978.

17 Labour Chamber of the Supreme Court May 14, 2000.

18 Public Interest Disclosure Act 1998.

19 Data Protection Act 1998.

20 *Durant v. Financial Services Authority* [2003] CA 1746 December 8, 2003.

21 The E.U. Member States plus Iceland, Liechtenstein and Norway.

22 Currently Switzerland, Canada, Argentina, Bailiwick of Guernsey and Isle of Man.

The authors may be contacted as follows:
 Mark E. Schreiber (mschreiber@palmerdodge.com);
 Jeffrey M. Held (jheld@palmerdodge.com);
 Robert T.J. Bond (rtjbond@faegre.com);
 Christian Runte (christian.runte@cms-hs.com);
 Raphaël Dana (www.soulier-avocats.com);
 Kate Flower (kateflower@eversheds.com).

For more information on *World Data Protection Report*, or to request a free trial, email marketing@bnai.com

Also available: *Sarbanes-Oxley Monitor*. Gain practical and expert help with how to comply with the Sarbanes-Oxley Act if you are a non-U.S. company listed in the United States. *Sarbanes-Oxley Monitor* is an online service, which helps you to understand how to comply. For more information or to request your free trial, email marketing@bnai.com