McDermott Will & Emery

An Employer's Guide to Implementing EU-Compliant Whistleblowing Hotlines

August 23, 2011

Under the Sarbanes-Oxley Act, companies listed on U.S. stock exchanges are required to establish a system, often called a "whistleblowing hotline," for employees to internally report concerns over questionable auditing or accounting matters. However, some European Union jurisdictions previously concluded that the EU privacy regime prohibited such hotlines. Over past few years, the EU and its Member States have articulated a framework for how to lawfully implement such a hotline throughout most of the European continent. This newsletter outlines a checklist of basic principles that multinational public company employers can follow to stay within this framework and mitigate the risk of an enforcement action on both sides of the pond.

Introduction

The corporate compliance, or "whistleblowing," hotlines required to fulfill obligations under the Sarbanes-Oxley Act of 2002 (SOX) do not sit easily within the framework of European Union data privacy laws. Regulatory decisions in France cast doubt on the legality of whistleblowing hotlines within the EU, and companies listed on U.S. stock exchanges appear to face a difficult choice between two seemingly contradictory regulatory regimes. This newsletter explains the current compromises enabling companies to satisfy requirements on both sides of the pond, and to meet their obligations under the law.

Background

In 2005 the French data privacy regulator, the CNIL, refused to authorize the creation of a SOX-compliant ethics hotline by McDonald's France on the grounds that to do so would violate French data privacy law. Of particular concern was the possibility that the submission of anonymous complaints could be abused in order to injure the reputation of coworkers, and that the hotline would lead to disproportionate data processing outside the EU of the personal data of French citizens. The decision caused some consternation among employers, to which EU-level and member state regulations have since responded.

The Article 29 Data Protection Working Party

In an attempt to provide a unified European position, the EU's standing working party on data transfer issues, the so-called "Article 29 Data Protection Working Party," produced an opinion in 2006. Although the opinion went some way to harmonizing the stance of data privacy regulators within the Member States, as explained below, multinational

companies may still have to engage in extensive background policy introduction work when putting into place measures to comply with SOX.

In the EU, personal data (*i.e.*, data by which an individual can be directly or indirectly identified) must be collected fairly and lawfully in order for the processing of that data to be legitimate. There are several grounds on which the collection and processing of such data can be lawfully collected (set out in the EU Data Protection Directive) and key among these for whistleblowing purposes are that the processing either must be necessary for compliance with a "legal obligation" to which the data controller is subject, or must be necessary for the purposes of legitimate interests pursued by the data controller.

The Working Party found that, while compliance with SOX was not capable of amounting to a "legal obligation" under the Data Protection Directive, adopting whistleblowing hotlines to prevent financial irregularity could be considered a legitimate interest of a company. Even a legitimate interest, however, may be overridden by the "interests for fundamental rights and freedoms of the data subject which require protection." The Working Party concluded that providing such protection means that the nature and scope of the hotline will need to amount to a proportionate means of achieving that interest and adequate data protection safeguards should be put in place.

The Working Party made a number of recommendations, principal among them being that any reporting should be done on a confidential basis, but by complainants who name themselves, and that the information collected should be restricted to accounting and auditing related matters.

The Working Party's opinion prompted a host of further local guidance from data protection regulators within the member states. Although the Working Party's opinion is not binding, it has proved very persuasive in member states. Companies expecting calls from or about employees in any such member states will need to understand both the Working Party recommendations and how they have been implemented in the relevant member states.

Local Guidance

Since the Working Party's opinion was released, Member State regulators have all adopted the Working Party's disapproval of anonymous reporting. While most regulators do not overtly prohibit anonymity, the overwhelming majority agree that it should be discouraged in favor of reporting on a confidential, named basis. A notable exception is the Portuguese Data Protection Authority, which goes as far as to say that anonymous reporting would not be permissible under Portuguese data privacy rules. On a Europe-wide basis, therefore, an employer's encouragement of anonymous reports seems unlikely to meet the principles of proportionality clearly set out in the opinion of the Working Party.

There is also a consistent position, in line with the Working Party's opinion, that whistleblowing hotlines, if introduced, should not replace existing internal reporting structures. German and French regulators in particular assert that hotlines should complement and not replace other internal processes designed to prevent fraud and corruption.

While the regulators are generally in agreement that only "SOX-type" reports are permissible within the scope of a whistleblowing hotline, German regulators are more relaxed in that reports pertaining to ethical considerations and human rights are also permitted. Some Member States place limits on who can be the subject of a report—in Austria, for example, only reports on management-level employees are permitted, and a similar recommendation exists in the Netherlands.

Considerations When Setting Up a Hotline

When setting up a SOX-compliant hotline in the EU, companies should consider adhering to these basic principles to avoid running afoul of EU requirements.

1. **Encourage "Confidential," Rather than "Anonymous," Reporting**: The practice of anonymous reporting should be discouraged. The explanatory materials distributed to EU employees regarding the hotline should make it clear that reporting should take place on a confidential, named basis.

2. **Set Up a Filtration System**: Inappropriate complaints should be filtered out at as early a stage as possible so they are not circulated. In particular, anonymous reports received despite discouraging materials should be treated with caution and only taken further when there is good reason to do so (*i.e.*, very serious allegations, for which it is apparent there is separate corroboration). Clear guidance should be given to those tasked with being the initial receiver of the report about when it will be appropriate to circulate further. A policy should be drafted to assist the initial decision-maker in exercising his or her judgment.

3. **Ensure Confidentiality and Data Security**: All reports should be submitted confidentially and the materials provided to employees should make this clear. The confidentiality of the information should be adequately safeguarded and electronic records should be password protected. Access to the data should be monitored and reviewed, while paper records should be kept physically secure. Employees assigned to investigate or consider complaints should be made aware of the importance of confidentiality and required to sign specific confidentiality agreements as necessary or appropriate.

4. **Limit the Nature and Scope of the Processed Data**: Only collect and process the minimum amount of data necessary for the purposes of complying with SOX. A template form for submission to be used by the whistleblower might helpfully be produced to ensure that only SOX-type complaints are

recorded. Consideration should be given as to who should be the subject of the report and what types of complaints can be made using the hotline. Companies that limit the scope of the hotline to SOX-type complaints are likely to be considered to be acting lawfully in this respect.

5. **Transfers of Data Outside of the EEA**: Transferring data outside of the European Economic Area (EEA) should only be done when absolutely necessary. Individuals should be appointed within each jurisdiction to deal with any reports that are made using the hotline. Specific internal procedures should be put into place to ensure the data, when transferred, is guaranteed a sufficient level of protection. Other measures, such as registering with Safe Harbor (a framework for EU-U.S. data transfers created by the U.S. Department of Commerce) or entering into transfer contracts based on the typical clauses issued by the European Commission in 2001 and 2004, will also protect against a breach of EU data protection law.

6. **Retention of Data**: Processed data should not be retained for any longer than is strictly necessary. In France, CNIL requires that information should not be retained for longer than two months after an allegation is found to be unproven. Where allegations lead to further proceedings, the data can lawfully be retained until the end of those proceedings. A retention policy should be drafted and rigorously applied in order to ensure that data is not kept for any longer than is necessary in the circumstances. Data that is retained for more than two months after a report is considered closed is likely to be considered unlawfully held.

7. **Ensure the Employee Is Given the Right of Correction**: The employee who is the subject of the report should be informed that the report has been made and given the chance to answer the allegations against him. This should be done as soon as the information is recorded, unless there are genuine concerns that protective measures need to put in place to preserve data. A specific policy should be put in place to cover the timing of informing the subject of a report, and a risk assessment might be devised to assist the decision-maker. Once the employee has been informed of the report against him, he or she should be allowed access to it and, if necessary, the opportunity to correct or clarify any incorrect or unambiguous data.

8. **Inform Employees**: Employees should be supplied with written materials explaining the operation and purpose of the hotline. Some jurisdictions (such as Germany and Austria) will require that the Works Councils are consulted before such lines are introduced. In any event, it is better from an industrial relations point of view to implement the hotline as transparently as possible, and informing employees prior to rollout of the line is advisable, even when not mandatory.

9. **Authorization Procedures**: Within each jurisdiction there will be different regulatory requirements to consider before rolling out a hotline. In France, for example, the hotline must be authorized by the CNIL, but it can take up to two months before a decision is made on noncompliant hotlines. A fast-track self-certification process exists for companies that adhere strictly to the CNIL's guidelines. This can be completed in two to three days, rather than the two to three months that can be expected when seeking express CNIL authorization. In any event, specific advice may be sought as to compliance with regulatory requirements when considering the timing of any rollout.

The Future

The Working Party has indicated it intends to publish another opinion on the issue of whistleblowing hotlines. There is no indication as to when that will be. What is clear, however, is that SOX and EU data privacy law will not easily be harmonized without considerable advance thought and preparatory work.

In addition, companies can go a long way toward mitigating the risk of an enforcement action under one or both schemes by taking a rigorous approach to the implementation and subsequent management of whistleblowing hotlines, which includes putting in adequate safeguards to ensure security, confidentiality and transparency in its operation. Companies are also wise to ensure compliance with any local recommendations by specific regulators where appropriate.

**Richard Cook, a trainee solicitor in London, also contributed to this article.*