Conflict of Laws: Anonymous Whistleblowing Hotlines under Sarbanes Oxley and European Data Protection Laws

RENZO MARCHINI

There has been much uncertainty as to the compatibility of U.S. whistleblowing schemes under Sarbanes-Oxley Act (SOX) with the EU data-protection rules. The EU Data Protection Working Party adopted an Opinion on the application of EU data-protection rules to internal whistleblowing schemes in the fields of accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crime. This article explains what prompted the Working Party to issue the Opinion and sets out the material points raised therein. The authors believe that the guidance provided is very useful in clarifying what is required to ensure full compliance with EU law, however, it does not completely eliminate the EU-U.S. confusion since the recommendations regarding the anonymity of whistleblowers do not match the SOX requirements.

A clash of approaches to the handling of anonymous whistleblowing systems was dramatically highlighted at the end of last year when a French court issued an order prohibiting McDonalds in France from continuing with their system on data-protection grounds.

As well as high-level discussions taking place between the U.S. and European officials, the Article 29 Data Protection Working Party (the Working Party), composed of representatives from each data-protection authority in the EU Member States, recently adopted its Opinion 1/2006 on the application of EU data-protection rules to internal whistleblowing schemes in the fields of accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crime (the Opinion). This article explains what prompted the Working Party to issue the Opinion and sets out the material points raised therein.

THE EU-U.S. PROBLEM

Companies operate internal whistleblowing schemes, such as reporting hotlines and websites, to encourage employees to report misconduct

Renzo Marchini is counsel in the London office of Dechert LLP. Mr. Marchini can be reached at *renzo.marchini@dechert.com.*

internally in order to ensure proper corporate governance. In some countries the functioning of whistleblowing schemes is provided for by law, while in the majority of Member States no specific legislation or regulation exists on the issue. However, whistleblowing schemes operating within the EU are likely to involve collection of personal data and so are required to comply with the EU data-protection rules enshrined in Directive 95/46/EC (the Directive), as implemented by the Member States (by the Data Protection Act 1998 in the U.K.).

In the United States, the Sarbanes-Oxley Act 2002 (SOX) requires publicly held U.S. companies and their EU-based affiliates, as well as non-U.S. companies listed on one of the U.S. stock markets, to establish "procedures for the receipt, retention and treatment of complaints received by the issuer regarding accounting, internal accounting controls or auditing matters; and the confidential, anonymous submission by employees of the issuer of concerns regarding questionable accounting or auditing matters" (Section 301(4)). This provision is mirrored in the Nasdaq and New York Stock Exchange rules.

As a result, there are EU-based affiliates of U.S. publicly held companies and EU companies listed on U.S. stock exchanges who are required to comply with both the Directive and SOX. In recent months there has been much uncertainty as to the compatibility of U.S. whistleblowing schemes with the EU data-protection rules. The companies concerned are facing risks of sanctions from EU data-protection authorities if they fail to comply with the EU rules, on the one hand, and from the U.S. Securities and Exchange Commission (the SEC) and the relevant stock exchanges if they fail to comply with the U.S. rules, on the other. This is demonstrated by the decision of a French court in September 2005 prohibiting a French subsidiary of McDonalds from establishing anonymous whistleblowing procedures on the grounds that EU data-protection law prevented the transfer of data without consent, thus placing the U.S. parent company in breach of SOX.

Despite the potential conflict between SOX and foreign law, the SEC has refused to grant exemptions or to state that the whistleblower requirements do not apply to non-U.S. entities. The Working Party is charged by the Directive to provide advice and guidance on its interpretation. The aim of the Opinion, issued on 1 February 2006, therefore, was to assess the compatibility of SOX-style internal whistleblowing schemes with the Directive and to clarify the requirements of the Directive so that companies, particularly those affected by SOX, can be clear as to what is required under EU law when implementing their schemes.

In recent months there has been much uncertainty as to the compatibility of U.S. whistleblowing schemes with the EU data-protection rules.

COMPATIBILITY OF WHISTLEBLOWING SCHEMES WITH EU LAW

For a whistleblowing scheme operating in the EU to be lawful, the processing of personal data needs to be legitimate and must satisfy one of a number of conditions set out in Article 7 of the Directive. Only two of the grounds in that Article appear to be relevant; the processing must either be necessary for compliance with a legal obligation (Article 7(c) of the Directive) or for the purpose of a legitimate interest pursued by the company to whom the data is disclosed (Article 7(f) of the Directive). The Working Party concluded that the legal obligation imposed by SOX, a foreign statute, to establish a reporting scheme does not qualify as a legal obligation capable of legitimising data processing in the EU. Whistleblowing schemes are, however, lawful in the EU on the

ground that they are necessary for the purpose of a legitimate interest pursued by companies, namely the facilitation of good corporate governance within those companies. However, Article 7(f) requires a balance to be struck between the legitimate interest pursued by a company processing personal data and the fundamental rights of the data subjects which has led to the Working Party's recommendations.

Incidentally, some Member States may well have to be justified on different grounds. In the UK, for example, information collected which may concern the alleged commission of an offence may well be characterised as "sensitive personal data" (the Directive does not deal with such classification), and so be subject to the additional controls applicable to that type of data under the UK's Data Protection Act 1998 (the DPA). In particular, the equivalent of Article 7(f) (namely, paragraph 6 of Schedule 2 of the DPA) is not available to justify the processing of sensitive personal data under the DPA. Nonetheless, other routes to justification are likely to be available.

As a general rule, the Working Party considered that only identified reports should be communicated using whistleblowing schemes. They suggested several reasons why anonymity might not be a good solution, for the whistleblower or the company.

KEY RECOMMENDATIONS OF THE WORKING PARTY

Limitations on the Use of Whistleblowing Schemes

Companies are recommended to carefully assess whether (a) a limit on the number of persons entitled to report alleged improprieties or misconduct through the whistleblowing scheme, and (b) a limit on the number of persons who may be incriminated through the whistleblowing scheme, is appropriate, in particular in light of the seriousness of the alleged offences to be reported. The Working Party also emphasised that whistleblowing schemes should be viewed as subsidiary to, and not a replacement for, other methods of internal management, such as employee representatives, line management and internal auditors. By contrast, under SOX, companies have flexibility in deciding who should receive reports made under schemes.

Restrictions on the Use of Anonymous Reports

As a general rule, the Working Party considered that only identified reports should be communicated using whistleblowing schemes. They suggested several reasons why anonymity might not be a good solution, for the whistleblower or the company, including that anonymity does not stop others from successfully guessing who raised the concern, it is harder to investigate if the company cannot ask follow-up questions to the whistleblower, and it is easier to organise the protection of the whistleblower against retaliation if concerns are raised openly. Whilst there would be exceptions to this rule, anonymous reporting should not be encouraged and, in particular, should not be advertised as a method of reporting under the scheme.

Companies should ensure that a potential whistleblower is aware that he will not suffer due to his action, that high levels of confidentiality are maintained, and that his identity may not need to be disclosed to people involved in any further investigation or subsequent judicial proceedings instigated as a result of his report. If a person still wishes to remain anonymous in these circumstances, an anonymous report can be accepted. However, the Working Party suggested that the appropriateness of anonymous reports be cautiously examined and that it may also be worth consid-

ering investigating anonymous reports with greater speed because of the risk of misuse. Under SOX, anonymity of whistleblowers is a statutory requirement. U.S. companies have flexibility in deciding how to ensure true anonymity and confidentiality.

Restrictions on Data Collection and Retention

Companies setting up a whistleblowing scheme should restrict them to reports concerning accounting, internal accounting controls or auditing or banking and financial crime and anti-bribery. The personal data processed within the scheme should be limited to the data strictly and objectively necessary to verify the allegations made. Data should only be kept for as long as is necessary, which will usually mean deletion within two months of completion of the investigation of the facts alleged in the report. Personal data relating to alerts found to be unsubstantiated should be deleted without delay.

Provision of Information about Whistleblowing Schemes

The Opinion requires companies to inform its employees about the existence, purpose and functioning of the scheme. In particular, employees should be aware of who receives the reports and the rights of access, rectification and erasure for reported persons. Companies should also provide information on the fact that the identity of the whistleblower shall be kept confidential and that abuse of the scheme may result in action against the perpetrator of the abuse. On the other hand, employees may also be informed that they will not face any sanctions if they use the scheme in good faith. Under SOX, companies have the freedom to decide how to effectively communicate the existence of schemes to their employees.

Rights of the Accused Person

The Working Party noted that existing regulations and guidance on whistleblowing focus on the need to protect whistleblowers and do not make any particular reference to the protection of the accused person. Even if accused, an individual is entitled to the rights he is granted under the Directive and the corresponding provisions of national law. Notably, the accused person has a right to be informed when personal data is collected from a third party on them as soon as practicably possible after data is recorded and of the alleged facts, unless this creates a substantial risk of jeopardising the company's ability to investigate the allegation or gather evidence.

Even if accused, an individual is entitled to the rights he is granted under the Directive and the corresponding provisions of national law. Notably, the accused person has a right to be informed when personal data is collected from a third party on them as soon as practicably possible after data is recorded and of the alleged facts.

Security of Processing Operations

A company must protect the data from accidental or unlawful destruction or accidental loss and unauthorised disclosure or access. The Working Party recommended that the means by which the data is collected should be solely dedicated to the whistleblowing scheme in order to prevent any diversion from its original purpose and for added data confidentiality (for example, dedicated email addresses for receiving reports). The objective of the whistleblowing scheme will only be achieved if the confidentiality of the whistleblower's identity and content of the report are guaranteed. The Working Party, however, noted that there may be an exception to the confidentiality of the whistleblower where he has

made a malicious false statement. SOX offers statutory protection for whistleblowers in publicly traded companies from retaliatory measures taken against them for making use of the schemes.

Management of Schemes

The Working Party favoured the internal handling of whistleblowing schemes. They recommended that management of a scheme be composed of specially trained and dedicated people, limited in number and contractually bound by specific confidentiality obligations. The scheme should be strictly separate from other departments of the company and complaint reports should be kept separate from other personal data. If a company chooses to use external service providers, the providers must be bound by a strict obligation of confidentiality and commit themselves to complying with the data principles. However, the company remains responsible for processing operations, and shall be required to periodically verify the compliance by external providers with the principles of the Directive. The U.S. rules are again flexible on the management of whistleblowing schemes and the SEC has recognised that the whistleblowing procedures adopted by audit committees should "fit" the company, according to its size and overall ethics programme.

Those new to European data protection may find much of the Opinion surprising.

Provision of Data to Other Countries

The nature and seriousness of the alleged offence should determine at what level and, therefore, in what country assessment of the report should take place. As a general rule, the Working Party believed that companies should deal with reports locally, i.e. in one EU country, rather than automatically share all the information with other companies in the group. Furthermore, a company should only transfer data to the U.S. (or any other third country which does not ensure adequate levels of data protection) where the intended recipient either participates in the U.S. Safe Harbour program, has contracted to provide adequate safeguards, or has a set of binding corporate rules in place which have been duly approved by the competent data-protection authorities.

THE SOLUTION?

The Working Party is confident that compliance with the Directive will help companies to ensure the proper functioning of whistleblowing schemes, whether they are obligatory schemes under SOX or otherwise.

Those new to European data protection may find much of the Opinion surprising. Why, they might ask, would a body charged with giving guidance in relation to compliance with data protection give advice to multinational companies in relation to such things as to whether having an anonymous hotline is in fact a "good solution" to their problems? Whilst much of the Opinion can be justified on the basis of giving guidance to such standard data-protection considerations as proportionate collection of data (must not be excessive), or duration of retention (not longer than necessary), there are parts which do seem to stray beyond that remit.

Nonetheless, when companies are setting up internal schemes in the fields of accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crime in the EU, they should pay close attention to the Working Party's recommendations, despite the fact that they are not binding.

The guidance provided is very useful in clarifying what is required to ensure full compliance with EU law, however, it does not completely eliminate the EU-U.S. confusion since the recommendations regarding the anonymity of whistleblowers do not match the SOX requirements.