Brussels, 3 July 2006
D(2006) MDF/ajv 8459

Mr. Ethiopis TAFARA
Director
Office of International Affairs
Securities and Exchange Commission
Washington, D.C. 20549
United States of America

Dear Mr. Tafara,

Thank you for your letter dated June 8, 2006 providing the Article 29 Working Party with the reaction of SEC staff on its Opinion adopted on February 1st, 2006, relating to the application of EU data protection rules to internal whistleblowing schemes in the fields of accounting, internal accounting controls, auditing matters, and the fight against bribery, banking and financial crime.

The Working Party appreciates your willingness to cooperate with it on this issue. It believes that this cooperation will help solve the concerns of US and EU companies that are bound to comply with SEC Rule 10A-3 and the requirements of Section 301 of the Sarbanes Oxley Act, on the one hand, and European rules on personal data protection, on the other hand.

The present letter is intended to provide clarifications on each of the points which you raised in your own letter dated June 8th. It confirms or completes the interpretation provided by Mr. Christophe Pallez, who met with you and other SEC representatives on March 8, 2006, in his capacity of Secretary General of the Commission Nationale de l'Informatique et des Libertés (CNIL), the French Data Protection Authority.

These comments follow the structure of your letter and should be read in conjunction with it.

1. *On the role of audit committees*

Paragraph A.1 of your comments requested clarification on how the role of audit committees and the ability of audit committees to provide information to the company's auditors or competent regulatory authorities could be affected by the Opinion.

In Section IV.6 of its Opinion, the Working Party introduced the principle that "groups should deal with reports locally, i.e. in one EU country, rather than automatically share all the information with other companies in the group". It also described two exceptions to this rule

This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.

The secretariat is provided by Directorate C (Civil Justice, Rights and Citizenship) of the European Commission, Directorate General Justice, Freedom and Security, B-1049 Brussels, Belgium, Office No LX-46 01/43.

Website: http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm

by providing that "the data received through the whistleblowing system may be communicated within the group if such communication is necessary for the investigation, depending on the nature or the seriousness of the reported misconduct, or results from how the group is set up".

This guidance derives from the essential data protection rule that personal data shall only be obtained and further processed for one or more specified and lawful purposes (Article 6.1(b) of Directive 95/46/EC). As a consequence, controllers should only communicate data to other entities, then qualified as "recipients", if the purpose for which the information was originally collected requires and justifies this communication. The exception mentioned in the third paragraph of Section IV.6 (iii) of the Opinion provides that this justification is in principle to be found in the nature of the communicated data. It also provides that this justification may be found, *as an alternative*, in the structure of the group.

The Working Party acknowledges that disclosure of a report to a few employees of another company or of other companies within the group may result from the organisation of the group, although this disclosure might not be strictly necessary for the investigation. This specifically refers to the possibility for groups to set up cross-functional management organisations for such reports, including individuals belonging to the various entities of a group, designated on the basis of their respective skills. Individual reports may be disclosed to those individuals based on their responsibilities. According to this exception, the Working Party believes that audit committees might be in a position to receive such reports, wherever they are located, when this communication is a natural consequence of the committee's tasks and functions. The same logic applies to company's auditors.

Furthermore, data controllers may communicate personal data to regulatory authorities when these authorities have the power to request such communication, by virtue of specific legal provisions. As a rule any access request by such regulatory authorities must be formulated *ad hoc* and should specify on which grounds it is based. This of course does not prevent data controllers from spontaneously informing the competent regulatory authorities in case of suspected improprieties of which these authorities should be informed, in accordance with their specific tasks and missions.

The Working Party therefore believes that EU data protection rules, as specified in the Opinion, do not prevent audit committees from being in a position to face their responsibility for oversight of whistleblower requirements under SEC Rule 10-A.

2. *Confidentiality and anonymity*

Paragraph A.2 of your comments requested clarification on whether the Opinion would discourage "confidential, anonymous reports" regarding questionable accounting or auditing matters, which would allegedly contradict the express requirement of Rule 10A-3 (ii).

The Opinion indeed deals at length with the question of whether whistleblowing schemes should make it possible to make a report anonymously rather than openly (i.e. in an identified manner, and in any case under conditions of confidentiality).

Article 6(a) of Directive 95/46/EC provides that "personal data must be processed fairly and lawfully". This requirement for fair processing applies in particular to the collection of personal data. In determining for the purposes of this principle whether personal data are

collected and processed fairly, regard is to be had to the method by which they are obtained. A risk exists, in this context, that anonymous collection of data is qualified as unfair collection of data. At any rate, the possibility to file anonymous reports can only increase the risk of frivolous or slanderous reports with the intention of causing the accused damage or distress.

I am personally keen to underline that this assessment must be read in the specific European context. It is certainly useful at this stage to recall that anonymous reporting evokes some of the darkest times of recent history on the European continent, whether during World War II or during more recent dictatorships in Southern and Eastern Europe. This historical specificity makes up for a lot of the reluctance of EU Data Protection Authorities to allow anonymous schemes being advertised as such in companies as a normal mode of reporting concerns.

However, neither data protection rules generally, nor the Opinion specifically, prevent anonymous reports from being filed through whistleblowing schemes. The Working Party further acknowledges, as the Opinion makes clear, that remaining anonymous might sometimes be the only available possibility for a whistleblower to raise a concern, who would otherwise risk being exposed to unacceptable physical or mental retaliation.

In this respect, the Working Party finds that it may take up the analysis made in a decision handed down by the US District Court of Columbia in April 2005 on the respective disadvantages and risks resulting from the possibility of a claimant initiating court proceedings under a pseudonym.[1] While the Court found that filing a request in an open manner "is an indication that the litigant's request is not frivolous and gets the case moving quickly", it also found that "a plaintiff's desire merely to avoid the annoyance and criticism that may attend any litigation is not sufficient to justify pseudonymous proceedings". However the Court also considered that in some cases "the need for anonymity outweighs (...) the risk of unfairness to the opposing party" and that "such critical or unusual cases may include those in which identification creates a risk of retaliatory physical or mental harm, those in which anonymity is necessary to preserve privacy in a matter of a sensitive and highly personal nature, and those in which the anonymous party would be compelled to admit criminal behavior or be subject to punishment by the state".

This is precisely the logic behind Section IV.2.iii of the Opinion, which is intended to reduce the cases in which anonymity might be used to convey slanderous or frivolous allegations on a specific person. The Opinion provides that "companies should not advertise the fact that anonymous reports may be made through the scheme". This implies that when first getting in touch with the scheme, a whistleblower should not be instantly offered the possibility to remain anonymous but rather the confidential nature of the scheme and the benefits of confidential reporting should be explained to them first. However, the report should still be taken by the scheme if this person wishes to remain anonymous, even after the advantages of identifying oneself have been explained to them.

Section IV.3 further provides that potential users of a whistleblowing schemes must be informed in a general manner "about the existence, purpose and functioning of that scheme". This general information would include the existence of the possibility to file anonymous reports through the scheme, as well as the fact that anonymous reports will be processed with

---

[1] David W. Qualls v. Donald Rumsfeld case (Civil Action No. 04-2113 (RCL)), April 27, 2005, available at the following address:
http://www.dcd.uscourts.gov/opinions/2005/Lamberth/2004-CV-2113~17:32:28~4-27-2005-a.pdf

specific precautions. This information should also make clear that the company prefers whistleblowers to identify themselves rather than remain anonymous.

The Working Party therefore confirms that the Opinion is not intended to direct companies to discourage or negatively characterise anonymous reporting when it is used to convey concerns which, if raised openly, would expose the whistleblower to unacceptable risks of retaliation. It is indeed intended to encourage companies to promote and favour identified confidential reporting over anonymous reporting, in the light of the various benefits to confidential reporting as listed in the Opinion.

3. *Classes of persons who can use the procedures and persons who can be subject of complaints*

Paragraph A.3 of your comments requested clarification on the classes of persons who can use the procedures and persons who can be subject of complaints.

The Opinion expressly provides that the Working Party has no wish to be prescriptive on either aspects of this issue and that "it leaves it to data controllers, with possible verification by the competent authorities, to determine whether such restrictions are appropriate in the specific circumstances in which they operate".

The Working Party believes that the Opinion provides data controllers with a very wide margin of manoeuvre to decide, if applicable, that their whistleblower procedures will cover all employees in all the fields covered in the Opinion.

4. *Data retention periods*

Paragraph A.4 of your comments requested clarification on the periods applicable to the retention of complaints.

The Working Party wishes to provide additional guidance on how long the reports filed through a whistleblowing scheme may be kept. Article 6.1(e) of Directive 95/46/EC provides that personal data must be "kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed."

The Opinion further provides that, as a rule, reports should be deleted promptly, and provides as a guideline the period of two months after the completion of the investigation of the facts alleged in the report.

This period will differ if legal proceedings or disciplinary measures are initiated against the incriminated person or the whistleblower (in cases of false or slanderous allegations). In such cases, personal data should be kept until the conclusion of these proceedings and the period allowed for any appeal. Such retention periods will be determined by the law of each Member State.

On the other hand, personal data relating to reports found to be unsubstantiated should be deleted immediately, without necessarily waiting for the end of the two-month period.

The Working Party acknowledges that data controllers may decide to archive rather than destroy the personal information mentioned on reports. Such a decision may be made upon an assessment of the risks incurred by the company for failing to keep a trace of the information internally, notably in terms of company liability.

Archiving means keeping the data in a separate information system with restricted access. This implies that once archived, the data is no more readily accessible in the working files of the persons dedicated to the processing of whistleblowing reports. It is accessible only on the basis of specific procedures regulating such access. Companies must implement appropriate technical and organisational measures to protect the archived data, in particular against unauthorised communication of, or unauthorised access to the data from within the company.

Access to the files of a sensitive nature should be limited to those within the company that have a genuine need to know given the reason for which the files were archived. Only the persons in charge of managing the whistleblowing scheme may request access to archives relating to previous cases handled by their internal organisation. Such access might be legitimate when it is required to defend the interests of the company in court, when it is necessary to comply with a request by an authorised third party (e.g. the judicial authorities investigating facts which might have been reported) or in cases when it is requested by the individuals identified in the reports in line with their statutory right to access and rectify data held on them subject to any relevant exemption.

The choice between destroying or archiving the reported data is the company's responsibility.

The Working Party hopes that these clarifications will prove useful. It believes that the current framework offers sufficient flexibility for companies to comply with both EU data protection rules and the requirement of Sarbanes Oxley relating to the "retention of complaints".

5. Additional matters

Finally Section B of your letter draws the Working Party's attention to additional matters which, although they do not directly pertain to the SEC's field of competence, the SEC wished to convey to the Working Party on behalf of multinational companies.

The Working Party shares the SEC's concern to prevent companies finding themselves in a situation where it would be impossible to comply with US and EU law on the one hand, or with different EU national standards, on the other hand, or where the costs of such international compliance would be truly excessive or disproportionate and could be avoided.

When it started dealing with the application of EU data protection rules to whistleblowing schemes, the Working Party chose to restrict the field of its work to Sarbanes Oxley-related matters as a matter of priority, so as to alleviate the risks that companies operating both in the US and in the EU could face risks of substantial sanctions either in the United States or in Europe.

The Working Party also indicated that it adopted its opinion on the clear understanding that it needs to further reflect on the possible compatibility of EU data protection rules with internal whistleblowing schemes in other fields than the ones just mentioned, such as human resources, workers' health and safety, environmental damage or threats, and commission of offences.

The Working Party will therefore consider during its next plenary meeting whether it is appropriate to provide additional guidance to companies on the application of EU data protection rules to whistleblowing schemes on matters falling outside the scope of its current opinion.

On behalf of the Working Party I wish to thank you and the SEC staff once more for sending us this detailed request for clarification. The members of the Working Party appreciate the quality of the relations between them and the SEC and firmly believe that this joint work, once made public, will be of assistance to companies operating both in Europe and in the United States.

With best regards,

Peter SCHAAR
Chairman

Cc: Mr. Jonathan Faull, Mr. Francisco Fonseca, (Justice, Liberty & Security DG)
Mr. Jurgen Tiedje, Mr. Philippe Pelle, M. P. Delsaux (Internal Market DG)
Mr. Dimitriou Dimitrios, (Employment DG)