Linklaters

One Silk Street
London EC2Y 8HQ
Telephone (44-20) 7456 2000
Facsimile (44-20) 7456 2222
Group 4 Fax (44-20) 7374 9318
DX Box Number 10 CDE

Office of the Secretary
Public Company Accounting Oversight Board
1666 K Street, N.W.
Washington, D.C. 20006-2803
E-mail address: comments@pcaobus.org

20 January 2004

Ladies and Gentlemen

Docket Matter No. 012
Proposed Auditing Standard on Audit Documentation
and Proposed Amendment to Interim Auditing Standards
Release No. 2003-023

We are submitting this letter in response to a request of the Public Company Accounting Oversight Board (the "**Board**") for comments in respect of its proposed audit documentation standard (to supersede AU. Sec. 339) and an amendment to the interim auditing standards (AU. Sec. 543) as directed by Section 103(a)(3)(A)(i) of the Sarbanes-Oxley Act of 2002 (the "**Act**").

We want, initially, to thank the Board for continuing to consider the position of foreign public accounting firms and the special concerns posed by application of certain aspects of the provisions of the Act and the Board's rules and regulations to such firms. We believe that the dialogue in which the Board has been engaging with many of its foreign counterparts has been constructive and we encourage the continued consideration of the position of foreign public accounting firms, particularly as regards their obligation to comply with the regulatory regimes in both their home jurisdictions as well as that of the United States.

We represent BDO Global Coordination B.V., Deloitte Touche Tohmatsu, Ernst & Young Global Limited, Grant Thornton LLP, KPMG International and PricewaterhouseCoopers International Limited, which are the co-ordinating entities of the international networks of the "Big Four plus two" accounting firms. We have been assisting our clients in relation to the non-US legal issues that arise out of the implementation of the Act, including issues connected with the proposed audit documentation standard (the "**Proposed Audit Standard**"), which remain of particular concern to our clients. Our clients have requested that we provide the Board with our analysis of one specific issue: the non-US legal data privacy issue that arises in consequence of the fact that audit documentation assembled and delivered to the auditor that issues the audit report in respect of an SEC-reporting issuer (the "**principal auditor**") pursuant to the Proposed Audit Standard may be disclosed to the Board or the US Securities and Exchange Commission ("**SEC**").[1] This issue is serious since there is a material conflict between the Proposed Audit Standard and the data privacy laws of many jurisdictions.

[1] This is not the only significant non-US legal issue associated with the Proposed Audit Standard. However, this letter does not consider any other issues.

The Proposed Audit Standard establishes general requirements for documentation auditors should prepare and retain in connection with any engagement conducted in accordance with auditing and related professional practice standards. In particular, the Proposed Audit Standard would generally require that audit documentation be retained at the offices of the principal auditor for a period of seven years from the date of completion of an engagement. Consistent with comments made by the Board and the Board's authority to obtain information under the Act, both we and our clients believe that one of the principal purposes of the proposal is to assist its efforts and those of the SEC to oversee and have the ability to inspect the work undertaken by non-US audit firms that audit the accounts of subsidiaries of US domestic companies whose securities trade in the US public markets. We also believe that a non-US court would be likely to consider this to be one of the principal purposes of the Proposed Audit Standard.

In a memorandum that our Firm submitted to the Board on 31 March 2003 entitled, *Legal Implications for Foreign Accountancy Firms in consequence of Registration with the PCAOB under the Sarbanes-Oxley Act of 2002* (the "**Memorandum**"),[2] we highlighted areas where there exist significant potential conflicts between the requirements of the proposed rules giving effect to the Act and the laws and regulations of a representative selection of jurisdictions[3] outside the United States. The Memorandum was primarily intended to identify and encourage consideration of the potential conflicts that would arise from completion of the Board's registration form by foreign public accounting firms that audit or play a substantial role in the audit of issuers (within the meaning of Section 2(a)(7) of the Act). The Memorandum focused in particular on conflicts arising in relation to confidentiality, data protection, legal enforcement, employment liability, banking secrecy and official secrets. Because we believe that the vast majority of the issues discussed in the Memorandum have equal application in the context of the Proposed Audit Standard, we do not propose to discuss in detail those issues again in this letter. However, we would commend the Board to review our Memorandum in order to more fully understand many of the non-US legal issues of concern to the Firms, as well as the data privacy and disclosure issues that are the focus of this letter.

As was the case with our Memorandum, we have not thought it necessary in connection with our consideration of the Proposed Audit Standard to conduct a comprehensive survey of all of the countries throughout the world that may be affected by this proposal. Instead, we have focused primarily on five countries, the United Kingdom, Germany, Spain, Brazil and Japan (the "**Surveyed Countries**") as well as the general European Union laws of data privacy. The Surveyed Countries were chosen not because they are known to be particularly difficult. Indeed, we have deliberately not chosen countries at the extremes in terms of ease (i.e. countries with no data privacy or other relevant laws) or difficulty (e.g. France and Belgium) on the grounds that these countries are not typical. Rather, we selected the Surveyed Countries on the basis that they are reasonably representative of the countries that are likely to be affected by the Proposed Audit Standard.

1 Basic legal impediments

The focus of this letter is data privacy laws since these are likely to impact most audits and a wider range of jurisdictions. It is important to note, however, that the issues arising under such laws are not the only issues associated with the Proposed Audit Standard.[4] The other issues can be broadly sub-divided as follows:-

---

[2] Please see http://www.pcaobus.org/rules/Comments_21-30_2003-001.zip for a copy of our Memorandum. A further copy is submitted with this letter as Appendix 1.

[3] These comprised the United Kingdom, Germany, Japan, Israel, Switzerland, Mexico and, in respect of certain issues, France and Brazil.

[4] For a more detailed discussion of these issues, please see our Memorandum.

(i) legal issues relating to professional duties and, in particular, duties of confidentiality; and

(ii) issues relating to various specific legal constraints (e.g. those arising under banking secrecy laws and national security laws).

In most jurisdictions (and specifically in each of the Surveyed Countries), duties of confidentiality are owed by an auditor to its audit client. In most jurisdictions, such duties can be waived under applicable law by that client but in some places (e.g. France and Belgium), waivers or consents cannot alter the legal duty.[5]

Under applicable non-US banking secrecy and national security laws, there may be circumstances in which an individual working for the auditor of the subject company could be entitled to have access to material protected by such laws in circumstances in which the Board or SEC would not be entitled to have such access because members of the Board or SEC do not have the requisite Governmental clearance to review such information.[6] In these circumstances, a disclosure of information with a view to its potential onward transmission to the Board or the SEC could be illegal.

These are clearly serious issues but they are not the subject of this letter.

2 Data privacy considerations

2.1 Duty of confidentiality

In many jurisdictions, personal data in the possession of a person (e.g. an audit client or an auditor) may only be used for a purpose that is deemed to be lawful. In particular, personal data may only be disclosed to a third party in circumstances falling within an exception to the general duty to preserve the confidentiality of such data.

The scope of this duty and the exceptions to it vary from jurisdiction to jurisdiction. At one extreme, there are countries (such as Brazil) that currently have no data privacy laws. At the other extreme, there are countries (such as Italy) that have extensive laws protecting all data whether relating to individuals or bodies corporate. The laws of most jurisdictions in those parts of the world where most relevant audit work is conducted, however, fall in between these extremes: they impose duties with regard to data relating to individuals. The jurisdictions that have data privacy laws now include many outside the European Union (e.g. Japan) but, since the relevant laws are generally no more extensive than those of Member States of the European Union, our focus will be on the laws of such Member States.

2.2 The basic issue

The foundation of the data privacy laws of all Member States is the European Union directive on data privacy (the "**Data Protection Directive**").[7] This permits "personal data" to be "processed" only if one of certain specified situations exist. Put broadly, the issue that concerns our clients is that audit documentation as defined by the Proposed Audit Standard[8] is likely to contain "personal data" within the meaning of the Data Protection Directive; the disclosure of such data to the Board or the SEC would constitute "processing"; but not all such disclosure would fall within one of the

[5] See paragraph 4 of our Memorandum for examples and further details.

[6] See paragraph 6 of our Memorandum for examples and further details.

[7] Directive 95/46/EC of 24 October 1995.

[8] See paragraphs 2 and 4 through 12 of the Proposed Audit Standard. Of course, a narrower definition of "audit documentation" might well result in it containing little or no personal data. This point is considered further in paragraph 4.1 below.

specified permissible situations. Hence disclosure to the Board or the SEC of all audit documentation is likely to be unlawful. Furthermore, because of this, it would be likely to be unlawful for an audit client or non-US auditor to assemble and deliver documentation to another third party (e.g. the principal auditor) in circumstances in which the onward disclosure to the Board or SEC was in contemplation.[9]

We will analyse the various elements of this problem in turn.

2.3 Personal data

The Data Protection Directive defines "personal data" to mean "any information relating to an identified or identifiable natural person".[10] The precise scope of this definition is unclear and there is currently no clear European Court guidance on its meaning. Furthermore, like all of the provisions of the European Union directives, the provisions of the Data Protection Directive do not have direct legal effect within the European Union. Each Member State has had to enact its own implementing legislation, and the result is inconsistency and still greater obscurity. What is clear is that European Union regulators and courts, in practice, have wide discretion to interpret the law, and their approach is likely to vary from country to country.[11]

The generally accepted legal view, however, is that the definition set out above should be construed broadly so as to encompass almost all information referencing an individual. In the context of workpapers maintained by auditors, this is likely to include information relating to a wide range of people: partners and employees of the local auditor; directors and employees of the audit client; individual customers and suppliers, and directors and employees of corporate customers and suppliers, of the audit client; and potentially others. Any audit document that mentions the name of any such individual potentially contains personal data.

2.4 "Processing"

The term "processing" includes "disclosure by transmission, dissemination or otherwise making available".[12] Clearly, therefore, disclosure to the Board or the SEC would comprise "processing". Hence, unless an exception were available, such disclosure would be illegal under the laws of European Union Member States.[13]

2.5 Exceptions

The most obvious exception to the prohibition on disclosure of personal data is the situation in which the individual to which the data relates has "unambiguously given his consent" to the disclosure.[14] This possibility is considered below.[15]

---

[9] This is not the only concern that arises under the Data Protection Directive in relation to disclosure or potential disclosure of personal data to the Board or the SEC but it comprises the most fundamental concern and hence is the focus of this letter.

[10] Article 2(a) of the Data Protection Directive.

[11] Spain, for example, has adopted a very narrow interpretation of the Data Protection Directive in its translation of the Directive into local law. As a result, it may well be that currently little data within Spanish audit documentation will cause concern. Furthermore, a very recent decision of the English Court of Appeal (*Durant v Financial Services Authority*, 8 December 2003) has given a restricted meaning to the term "personal data" under UK law. This decision shows commendable common sense, but it is out of line with the interpretation given to the relevant local law by most of the European regulators (including the normally liberal UK Information Commissioner, who is having to reconsider his position and published guidance in the light of the decision).

[12] Article 1(b) of the Data Protection Directive.

[13] Assuming each Member State has properly implemented the Directive, which most have in this respect.

[14] Article 7(a) of the Data Protection Directive.

[15] See paragraph 3.3 of this letter.

The only other situations in which disclosure is permitted and which might at first sight be of assistance in the present case are situations in which either:

(i) "processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed";[16] or

(ii) "processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for (*sic*) fundamental rights and freedoms of the data subject which require protection under [the Data Protection Directive]".[17]

Once again, it is impossible to define precisely the scope of these exceptions and of the relevant implementing laws of Member States and there are no decisions of relevant appellate courts that materially assist in their interpretation. However, the generally accepted view is that general disclosure of all personal data in audit documentation to non-European Union regulators (such as the Board and the SEC) is not permitted by these exceptions. We share this view and, more importantly, so do the key European Union regulators.[18]

2.6 Indirect securing of illegal objective

In the absence of consent from the relevant data subjects, the disclosure of all audit documentation to the Board or the SEC would be likely to be illegal under the laws of Member States of the European Union. The Proposed Audit Standard, however, does not by its terms require disclosure to the Board or the SEC: it requires disclosure to the principal auditor. It is, therefore, necessary to consider whether this alters the above analysis.

In our opinion, it does not. Yet again, it is possible that the laws of different Member States may differ and there is no clear judicial guidance. However, under the laws of those jurisdictions that we have specifically considered for this purpose (i.e. Germany and the UK), we believe that a disclosure of data to a principal auditor pursuant to the Proposed Audit Standard would be regarded as having as one of its purposes the assistance of the Board and the SEC in their investigations and the enforcement of the Act and other applicable laws and that, in consequence, such disclosure would be regarded as a matter of law in substantially the same manner as a disclosure to the Board or the SEC itself.[19] This is consistent with the normal requirement that European Union directives and laws implementing them be interpreted purposively[20] and also with the essentially purposive language of the relevant parts of the Data Protection Directive and the relevant implementing legislation.

---

[16] Article 7(e) of the Data Protection Directive.

[17] Article 7(f) of the Data Protection Directive.

[18] In any event, the exceptions do not extend to sensitive personal data (e.g. the disclosure of medical data or information relating to criminal convictions). Furthermore, several Member States of the European Union have not enacted the relevant exceptions in full or even at all. Spain is one such Member State. See further paragraphs 3.3.2 and 3.3.5 of our Memorandum.

[19] Japanese law may differ slightly in this respect in that we have been advised that the privacy problem might arise not at the time of the disclosure to the principal auditor but in the event of a subsequent disclosure to the Board or the SEC.

[20] Case C – 84/95 *Bosphorus* v. *Minister for Transport, Energy and Communications, Ireland and the Attorney General* [1996] ECR I-3953 and Case C - 6/72, *Europemballage Corporation and Continental Can Company Inc.* v. *Commission of the European Communities*. [1972] ECR I-157.

3 The disclosure problem in practice

3.1 US firm conduct of audit work

One option that we understand has been suggested with a view to overcoming the problem identified above is for the US firms (or other principal auditors) to send audit teams to the relevant non-US jurisdictions to undertake the necessary audit work and then assemble and retain all relevant audit documentation. However, this would not solve the problem described above. The precise legal analysis would differ by country, but the end result would be that data would have to be disclosed to the relevant US firm knowing that it would be assembled and retained with a view to its potential disclosure to the Board and the SEC. This would be likely to be unlawful in most European Union jurisdictions.[21]

3.2 Redaction of personal data

The data privacy problem is caused by the presence of personal data in audit documentation. Consequently, although highly theoretical, under applicable data privacy law the problem could be solved by the redaction of that documentation so as to remove all personal data. However, we suspect that the costs and time that would need to be devoted to a redaction exercise of this kind would be so huge as to render the process impracticable.

As this letter suggests, data privacy law is extremely complicated, and analysing all audit documentation with a view to ensuring that data that is protected by local law (but only such data) is eliminated from the audit documentation would be a very time consuming and subjective process. As we have previously indicated, audit workpapers are likely to contain a considerable range of personal data. Redaction would literally involve the analysis of each and every workpaper and, in many cases, the production of versions of documents with names and other details omitted. This might be a practical solution in connection with a one-off request for specific audit workpapers. The burden of compliance in such a case would be limited and could doubtless be further limited after discussion with the Board or SEC on a case-by-case basis. In relation to the Proposed Audit Standard, however, the compliance burden would exist in relation to each and every audit document relating to any audit of an SEC-registrant, and there would be no meaningful opportunity to discuss how to address any specific problems.[22]

The consequence of this is that, although it is essential that the Proposed Audit Standard state that the obligations imposed by it are subject to applicable foreign law if a conflict with non-US laws is to be avoided, it is by no means sufficient in and of itself to deal with the practical problems that are likely to be encountered.

3.3 Securing consents from affected data subjects

Certain data privacy and other problems can, of course, be overcome by obtaining the consent of the third party to whom a duty of privacy is owed.[23] It is, therefore, necessary to consider whether consents might be obtained so as to solve the problem considered in this letter. Unfortunately, this would not be possible for several reasons.

---

[21] We have not been asked to consider in this letter other potential local law issues with this suggestion (e.g. the lawfulness of the conduct of local audit work by the US firms under local audit licensing laws).

[22] The existence of a specific request made in relation to a specific investigation or enforcement action might also enable reliance to be placed on exceptions to the duty of confidentiality that would not be available in relation to the kind of general disclosure contemplated by the Proposed Audit Standard. Hence, the amount of data required to be redacted in relation to a disclosure under that Standard might be greater than the amount required in relation to a specific request.

[23] See, for example, Article 7(a) of the Data Protection Directive.

First, and most obviously, the number of data subjects is likely to be so large that obtaining consents from all of them would be logistically almost impossible.[24] Many would have no incentive even to reply to a request for consent and others might well refuse consent on principle.

Equally seriously, many consents would be effectively void. This is because the relevant consents must normally satisfy some basic requirements. Under European Union law, for example, they must be "freely given, specific and informed".[25] Hence, it is not always possible to obtain effective consents, particularly from employees, nor is it always practicable to do so.[26] In any event, in many jurisdictions, consents are revocable at any time.

The problem with the Proposed Audit Standard is that any consents would have to deal with future data of a non-specific nature. Consequently, subject to what is said below, in many places, including most jurisdictions within the European Union, no meaningful or reliable consents could be obtained in advance as they would not be "specific and informed".

In some jurisdictions, it would be possible to obtain effective consents from members of the non-US firm's audit team (i.e., the partners and staff engaged on the relevant audit), provided that these consents were sought around the time when the audit work commenced and, probably, that the giving of the consent was a condition of being permitted to be a member of the team. This process would obviously be cumbersome, but it would at least resolve one of the data privacy issues.

Another meaningful consent that could be obtained in advance in relation to audit documentation is the consent of the relevant client. We note in this context that another possible way of progressing this might be through an SEC rule requiring SEC-registrants to consent or procure that their subsidiaries consent to the production of relevant documentation.

As indicated above, however, these consents would only scratch the surface of the problem. The data privacy issue would remain in relation to all other personal data in the audit documentation.

4 Overcoming the problems

It is not easy to find a legally acceptable and practical solution that would be applicable in most jurisdictions to the problems described above and the problem is compounded by the concern that regulators outside of the United States may look at the substance of what is occurring (i.e. the delivery of data to a non-European Union regulator) rather than at its form. Nonetheless, there are various possibilities that may be worth exploring further.

4.1 Limiting the content of

The problem discussed in this letter is caused by the existence of "personal data" within audit documentation. As indicated above, this typically comprises information relating to "an identified or identifiable natural person".[27] If the Proposed Audit Standard were to restrict the scope of the materials that the Board requires be assembled and delivered to the principal auditor to something likely to contain significantly less information about individuals, then the data privacy problem

[24] See paragraph 2.3, which considers the range of individuals from whom consent might be required.

[25] Article 1(h) of the Data Protection Directive.

[26] Under the laws of most European jurisdictions, it is almost impossible to assert that a general consent given by an employee is "freely given".

[27] Article 2(a) of the Data Protection Directive. As indicated above, some states, such as Italy, have extended their data privacy laws to encompass data relating to corporations.

would at the very least be greatly reduced in scope. Clearly, the more limited the scope of such materials, the less difficult the problem would become.

4.2 Use of other regulators

In general, the laws of most EU Member States permit the disclosure of personal data to local regulators for specific investigatory and monitoring purposes pursuant to the "public interest/official authority" provisions of the Data Privacy Directive.[28] Furthermore, the same provisions would normally enable the non-US securities regulator to cooperate with the SEC via the IOSCO Memoranda of Understanding in relation to investigations and enforcement matters. This fact may be crucial in assessing the impact of some of the possible changes to the Proposed Audit Standard and considering their acceptability from a policy perspective. For example, the impact of the maintenance of audit documentation by the local auditor within the relevant non-US jurisdiction rather than by the principal auditor in the United States of America should be viewed in the light of the ability of the non-US securities and/or accounting regulator to access that documentation. In addition, the position of the Board could be further enhanced if it were to enter into cooperation agreements with the relevant non-US accounting regulators in relation to enforcement and investigations. These ideas reflect some of those outlined by the Board in its *Proposed Rules Relating to the Oversight of Non-U.S. Public Accounting Firms*, dated 10 December 2003,[29] and we would commend the Board to consider the issues raised above in light of that proposal and its implementation.

We recognise that the legal and administrative difficulties to be addressed before any solution can be reached will be considerable, and that there will be many second-order issues that will need to be overcome (e.g. in relation to employee and customer notifications and sensitive data). In practice, in many countries, the attitude of the non-US regulator will be crucial, and non-US regulatory objectives and policy as much as law will then determine the outcome of any discussions. We believe that the dialogue that is underway between the Board, the Firms and non-US regulators, particularly within Continental Europe, will be key to resolving these issues in a manner that best achieves the goals of the Board, while recognising and taking into account the foreign law issues resulting from the proposed rules.

* * * *

We would be pleased to respond to any inquiries regarding this letter or our views on the Proposed Audit Standard generally. Please feel free to contact either Richard Godden or Jason Manketo in London on +44 207 456 2000.

Very truly yours

Linklaters

Linklaters

[28] Article 7(e) and Article 13(f) of the Data Protection Directive. Sensitive personal data, as always, would remain a problem, but in many cases a way around the problem could be found, particularly if the derogation powers in Articles 8(4) and 8(5) of the Data Protection Directive are utilised. However, this would require action by EU legislators or regulators, as non-EU regulators cannot take advantage of these provisions.

[29] Docket Matter No. 013, Release No. 2003-024.

Appendix 1

Linklaters

Memorandum

31 March 2003

To	Office of the Secretary of the PCAOB
From	Linklaters
Direct Line	020 7456 2750

Legal Implications for Foreign Accountancy Firms in consequence of Registration with the PCAOB under the Sarbanes-Oxley Act 2002

1 Introduction

We have been instructed by the Big Four accountancy firms (the "**Firms**") to draft a report highlighting areas where there are significant potential conflicts between the requirements of the proposed rules giving effect to the Sarbanes-Oxley Act 2002 (the "**Act**") and the laws and regulations of jurisdictions outside the United States (the "**Report**"). These potential conflicts arise from the requirement for Firms which carry out audit or audit related work on behalf of companies which have reporting obligations to the Securities and Exchange Commission (the "**SEC**") to register with the Public Company Accounting Oversight Board (the "**PCAOB**") and to comply with the rules and regulations imposed by the PCAOB, pursuant to the provisions of the Act.

This memorandum is intended to address the PCAOB's request in its Release No. 2003-1 dated 7 March 2003, for potential conflicts to be identified.

In the time available, it has not been possible to conduct a comprehensive review of a large number of territories affected by the Act. A more limited survey has therefore been undertaken, focusing on a representative cross-section of territories in order to provide the PCAOB with an indication of some of the significant issues with which the Firms are faced. The jurisdictions that participated in our review are the United Kingdom, Germany, Japan, Israel, Switzerland, Mexico and, in respect of certain issues, France and Brazil.

We have considered each area of potential conflict, highlighting legal restrictions which create obstacles to the compliance of Firms outside the United States with the obligations of the Act and examples of sanctions that will be applicable where such restrictions are breached. Potential exceptions which may legitimise compliance with the Act's requirements have also been identified. Clearly, we would expect that further work and dialogue between relevant authorities will be required to resolve potential conflicts.

2 Executive Summary

2.1 There is significant potential conflict between the Act and the laws and professional regulations within those jurisdictions surveyed, including in relation to data protection, confidentiality,

employment, bank secrecy and the extent to which a foreign legal obligation can be enforced. The effect of this would be to prevent full compliance with the requirements which the Act places on Firms to disclose information upon registration with the PCAOB or pursuant to requests for testimony or the production of documents made by the PCAOB[1].

2.2 The conflicts identified can be summarised as follows:

2.2.1 **Confidentiality** – all of the jurisdictions raised issues of confidentiality. The duty of confidentiality between a Firm and its client is very strict and places significant restrictions on a Firm disclosing any client or third party information which has become known to it during the course of business. Furthermore, a duty of confidentiality also arises in the context of disclosure of employee data.

2.2.2 **Data Protection** – data protection legislation in some of the jurisdictions surveyed prohibits the disclosure of personal data to the PCAOB and the transfer of such data into a jurisdiction which is not considered to have an equivalent level of data protection, unless relevant exceptions apply.

2.2.3 **Legal Enforcement** – all of the jurisdictions raised issues in relation to the PCAOB conducting inspections of a Firm's operations and practice. These issues relate to national sovereignty and consequential restrictions on extraterritorial enforcement of foreign legal obligations.

2.2.4 **Employment Liability** – some of the jurisdictions raised employment liability issues in relation to the requirement under the Act for Firms to agree to secure consent from all associated persons regarding compliance with requests for testimony. In particular, these issues will arise where a Firm makes it a term of an employee's employment to provide such consent, it being a ground for dismissal where they refuse.

2.2.5 **Banking Secrecy** – some of the jurisdictions have banking secrecy legislation which requires banks, their officers and employees to keep secret the identity of their clients and details of their relationship with them. This raises particular concerns where a Firm has banking clients.

2.2.6 **Official Secrets** – some of the jurisdictions have rules that exist to protect national security which prevent unauthorised disclosure of certain information to protect the state from espionage. In such cases, conflicts with the Act will arise where a Firm has in its possession documentation of relevance to national or economic security.

[1] Section 102 (b) (3) of the Act

2.3 Most of the relevant jurisdictional laws and regulations are expressed in general language, in particular the various exceptions to provisions which conflict with the Act's requirements. The existence or extent of a conflict will to a large extent depend on how such language is interpreted. A sympathetic court or regulator may use the flexibility provided by such general language to reconcile any potential conflict between the local and United States requirements. Conversely, a court or regulator that was not so predisposed may find a real conflict. Simply relying on these potential interpretations raises risks which are not insignificant. These risks include exposure to criminal and civil liability.

2.4 Obtaining express consent from relevant individuals may provide a way around the potential conflict between the United States and local requirements to the extent that such requirements arise in relation to Firms' clients, who would presumably give their consent. However, consent only deals with some of the issues and does not provide a means of overcoming all conflicts:

2.4.1 in France, for example, prior consent of the client would not release a Firm from criminal and civil disciplinary sanctions where they breach obligations of client confidentiality;

2.4.2 in Switzerland, prior consent of a client would not release a Firm from criminal liability where they are in breach of the anti-espionage legislation, which is broadly applied, making it an offence to make available business information to a foreign authority where it is deemed not to be in the interests of the Swiss Confederation;

2.4.3 in some jurisdictions, such as the United Kingdom, Germany and Japan, consent given by certain individuals, especially employees, may not be valid and in the United Kingdom and Germany would not in any event override the privilege against self-incrimination;

2.4.4 the PCAOB, as a result of its broad powers under the Act, may request the disclosure of or, in the course of an inspection, become aware of information which contains personal details relating to individuals not connected to clients who are SEC registrants or issuers and who would not therefore be similarly motivated to consent to the disclosure;

2.4.5 in some territories (for example, Switzerland) restrictions on extraterritorial enforcement of legal obligations cannot be overcome by consent of the Firm.

Similarly, drawbacks exist in relation to other potential exceptions including disclosures made in the public interest or required by a legal obligation.

2.5 In light of these conclusions, it seems desirable that the Firms discuss these matters further with relevant government and regulatory bodies in the United States and in their respective jurisdictions in order to identify an acceptable way forward.

3 Data Protection

3.1 Restrictions

Many of the jurisdictions we surveyed have data protection or privacy legislation in place which will pose significant restrictions on a Firm's ability to disclose information to the PCAOB.

Essentially, data protection legislation seeks to regulate the use of "personal data",[2] which means data (this may include electronic and manual data) relating to an identifiable individual (a "data subject"). The various laws impose certain obligations on an entity which collects and controls the use of the personal data ("data controller") and, more importantly in the context of the Act, there are significant restrictions on who that personal data can be disclosed to.

Data Protection legislation in the European Union is based on the Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data (95/46/EC) (the "**EU Data Protection Directive**"). The EU Data Protection Directive has been implemented in the various EU member states in broadly the same fashion, although it is worth noting that significant variations exist between member states that are free to implement stricter requirements if they wish.

Data protection legislation is not limited to the EU and there are many other jurisdictions that have legislation setting out similar requirements to the EU Data Protection Directive, such as Switzerland[3], Israel[4], Japan[5] and Hong Kong[6].

The most significant restrictions imposed by data protection legislation can be summarised as follows:

3.1.1 Restrictions on Disclosure

Disclosure of personal data to the PCAOB is prohibited unless a relevant exception applies (see further paragraph 3.3 below). This raises potential conflicts with the requirements under the Act including those which:

(i) compel registrants to provide a list of all accountants associated with the Firm who participate in or contribute to the preparation of audit reports including the person's name, social security number (or comparable non-United States identifier), and all license or certification numbers authorising the person to engage in the business of auditing or accounting[7];

(ii) compel registrants to reveal information relating to criminal, civil, or administrative actions or disciplinary proceedings pending against any associated person of the Firm in connection with any audit report[8];

(iii) allow the PCAOB to demand from the registrants any other kind of information that the PCAOB has specified as necessary or appropriate in the public interest or for the protection of investors[9]; and

---

[2] In many jurisdictions personal data covers only data relating to identifiable living individuals, however, it is worth noting, that there are some jurisdictions, outside the scope of this submission that also regulate the processing of data relating to legal entities, for example, Italy.

[3] Federal Act on Data Protection 1992.

[4] The Privacy Protection Law 1981.

[5] Japan is currently implementing data protection legislation. Our analysis is therefore based on the provisions of the draft legislation.

[6] The Personal Data (Privacy) Ordinance.

[7] Section 102 (b) (2) (E) of the Act.

[8] Section 102 (b) (2) (F) of the Act.

[9] Section 102 (b) (2) (H) of the Act.

(iv) entitle the PCAOB to require Firms to report more frequently than in its annual report in order to update its application and other information concerning the Firm and all accountants associated with the Firm[10].

The disclosure requirements of the Act relate to employees, clients and third parties. Although certain information relating to the Firms' clients is not required per se as part of the process of registration with the PCAOB, the Firms are compelled to give their consent to co-operate in and comply with all requests for testimony or the production of documents made by the PCAOB[11]. Such documents or information may relate to the Firms' clients or third parties, for example, copies of audit work papers. To be able to give such consent the Firms need to be in a position vis-à-vis their clients and any other third parties to justify such co-operation and disclosure.

It is clear from our survey that the disclosure of the information required by registration or in connection with the ongoing oversight of the PCAOB will be significantly restricted by data protection requirements in certain jurisdictions.

In the United Kingdom the first principle of the Data Protection Act 1998 ("DPA") requires that personal data be processed fairly and lawfully. To this end the disclosure of information to the PCAOB will only be permissible if one of the exceptions identified in paragraph 3.3 below apply. This is also the case under the German Data Protection Act 1990 (as amended in 2001).

Data which is classified as "sensitive personal data", pursuant to the EU Data Protection Directive, attracts a higher degree of protection from disclosure and the relevant exceptions are generally more difficult to satisfy (see further paragraph 3.3 below). The requirement under Section 102(b)(2)(F) of the Act to disclose information relating to offences or alleged offences or disciplinary proceedings will be categorised as sensitive personal data whether or not they are in the public domain.

3.1.2 Restrictions on Transborder Data Flow

Transfer of personal data to a jurisdiction which is not considered to provide an equivalent level of data protection is prohibited unless a relevant exception applies (see further paragraph 3.4 below). Of the territories surveyed, the United Kingdom, Germany, Switzerland and Israel[12] place such restrictions of the transfer of data outside their jurisdiction to the United States, which is not considered to have an equivalent level of data protection for these purposes. Similar restriction apply in respect of all EU Member States, Poland, Hong Kong and Canada.

3.2 Sanctions

Breaches of data protection legislation attract both criminal and civil sanctions, including exposure to regulatory fines and individual claims for damage and distress. In the United Kingdom, for example, a person would be criminally liable where they breached the Data Protection Act 1998 and failed to comply, or falsely purported to comply, with an enforcement notice issued by the

---

[10] Section 102 (d) of the Act.

[11] Section 102 (b) (3) of the Act.

[12] The Privacy Protection (Transfer of Data Outside of Israel) Regulations 2001 set out this requirement for the transfer of *databases* outside Israel. Although information held by Israeli accountancy firms and requested by the PCAOB is unlikely to be classified as a "database" for these purposes, it is reasonable to assume that similar criteria will be applied by Israeli courts regarding the transfer of sensitive data outside Israel.

Information Commissioner to remedy the breach. In Switzerland, a person who wilfully and without authority discloses sensitive personal data can be punished by fine or imprisonment[13]. The legislation in Germany and Spain also provides for criminal sanctions.

In addition, regulatory fines can be substantial. Although Spain is not one of the jurisdictions we surveyed, we are aware that the Spanish Data Protection Agency imposed a fine on Telefonica Espana of €840,000[14].

3.3 Exceptions to Restrictions on Disclosure

The most relevant exceptions to the restrictions outlined above are:

3.3.1 Consent

Consent of the "data subject" in all the jurisdictions surveyed would permit Firms to disclose the requested data to the PCAOB without breaching the relevant data protection legislation.

In relation to the disclosure of "sensitive personal data", obtaining the explicit consent of the relevant individual is the only relevant exception.

The consent is not required from the corporate client[15] but from each and every individual whose data is contained in the information to be revealed to the PCAOB.

Whilst it may be expected that clients who are SEC registrants or issuers would readily consent to the disclosure of their data to the PCAOB, it should be noted that:

(i) the PCAOB, as a result of its broad powers under the Act, may request the disclosure of or - in the course of an inspection - become aware of information which contains personal details relating to individuals not connected to the SEC registrant or issuer clients and who would not therefore be similarly motivated to consent to the disclosure. This information may, for example, be contained in audit work papers. Obtaining the consent of all clients/third parties, including non-SEC listed clients/third parties would be a logistical challenge, if not practically impossible in some circumstances;

(ii) gaining the consent of an issuer with whom a Firm has played a substantial role, rather than the main role, in respect of preparing or furnishing them with an audit report is also likely to be logistically challenging;

(iii) even if given, consent can be withdrawn at any time;

(iv) Firms are unlikely to have obtained the consent of certain data subjects, such as its employees, particularly given that most data collected about them will have occurred prior to the implementation of the Act. It is clear that obtaining such consents will involve substantial effort. For example, the information required by the PCAOB on criminal convictions in connection with audit reports relating to the

---

[13] For these purposes sensitive personal data will be data relating to religion, political beliefs, trade union activities, health, race, social assistance or criminal records.

[14] A subscriber had opted out of the use of his data for anything other than the provision of the telephony service for which he was subscribing. Despite this, Telefonica Espana proceeded to share that individual's data with one of its subsidiaries, Telefonica Data and the individual in question then reported Telefonica Espana to the Spanish Data Protection Agency.

[15] Except where personal data is defined to include corporate data, such as under Italian data protection laws.

Firm or "any person associated with" the Firm and dating back 10 years[16], may pertain to a large number of individuals;

(v) there is a real risk that in certain circumstances consent may not be regarded as legal, especially where such consent is required of employees. For consent to be valid, it must be freely given. For example, in accordance with the EU Data Protection Directive, the relevant United Kingdom and German implementing legislation requires that the consent must be "freely given, specific and informed".

Obtaining consent in the employment context – for example, from a Firm's employees – may be difficult to establish. In the United Kingdom and Germany, in accordance with the Article 29 EU Data Protection Working Party[17], it has been questioned whether consent given in an employment context constitutes "freely given consent" as employees do not have the option to refuse their consent without possible adverse consequences.

It also remains questionable how a client's consent can be freely given if, without such consent, a client would not be able to retain a registered Firm.

It remains unclear how this requirement of "freely given consent" will be interpreted in respect to the disclosure obligations by accountants under the Act and whether the United Kingdom and German regulators will choose to take a pragmatic view of consents given by such highly-remunerated, well-informed employees and consider them to be legitimate. There has been no official view disclosed by regulators in either jurisdiction in this respect; and

(vi) in relation to "sensitive personal data", it may be even more difficult to obtain valid consent in circumstances where potentially incriminating activities are being investigated: individuals are less likely to willingly consent to the disclosure of information relating to criminal actions pending against them.

3.3.2 Public Interest

The United Kingdom and Israel will allow disclosure of personal data to the PCAOB where the processing of such data is in the public interest. However, the interpretation of what is in the public interest is a question for the regulators and courts in each jurisdiction to decide.

It may be felt that this exception can be relied upon to legitimise the disclosure and inspections required by the Act in view of, amongst other things, the "public interest" nature of the Act and the harm it is intended to counter. However, to date "public interest" has been narrowly construed and it is unclear whether the obligations under the Act will be interpreted as being in the public interest of the local territory as well as the United States.

In the United Kingdom, for example, disclosure may be permitted where it is necessary "*for the exercise of any functions of a public nature exercised in the public interest by any person*" where a Firm can show that it is exercising a function of a public nature in the public interest. The definition of public interest has to date been narrowly interpreted by

[16] Part V, item 5.1 of the PCAOB's proposed rules.

[17] The working party set up pursuant to Article 29 of the EU Data Protection Directive. It is an independent advisory body whose opinions are not legally binding.

the United Kingdom regulators and courts[18] and there is no precedent for this exception being successfully relied upon in circumstances such as these.

Use of this exception in Israel is also questionable given that the public interest arguably relates to that of another jurisdiction.

As such, it remains unclear whether this exception can be relied on.

3.3.3 Compliance with a legal obligation

The data protection legislation in the United Kingdom, Germany, Israel and the draft data protection bill in Japan provide for disclosure of personal data where it is necessary for compliance with any legal obligation to which a Firm is subject.

However, this exception will not apply to foreign (in this case, United States) legal requirements. The Israeli Interpretation Law 1981 provides that this exception can only be defined as applying to an Israeli legal obligation and, similarly, under the Draft Data Protection Legislation in Japan, a legal obligation will not include that of a foreign jurisdiction. Likewise, United Kingdom and German Data Protection Legislation makes it clear that this exception will only apply to local legal obligations.

3.3.4 Whilst it may be felt that a court or regulator in the relevant jurisdiction would strive to reconcile a potential conflict between United States and local laws and recognise United States legal requirements, it must be recognised that a court or regulator may find it difficult to do so without opening the floodgates to laws of other jurisdictions

3.3.5 Legitimate Interests

In the United Kingdom and Germany, in accordance with the EU Data Protection Directive, disclosure is permitted if it is necessary for the legitimate interests pursued by a Firm or by the third party or parties to whom the data is disclosed, except where the processing is unwarranted in any particular case by reason of being overridden by the rights and freedoms or legitimate interests of the individual.

It may be deemed surprising, in the current circumstances, that certain disclosures will be overridden by the rights and freedoms or legitimate interests of the data subjects. However, the United Kingdom or German regulator or court may take a different view. For example, blanket disclosures of information relating to disciplinary actions (however small) pending against a Firm or associated person would undeniably be prejudicial to an individual who had committed a disciplinary or other offence.

Each individual case would need to be considered on its own facts to determine whether an overriding interest of the data subject exists, prohibiting that particular disclosure of personal data. With this in mind it is clear that this exception may well enable disclosure in certain circumstances but could not be used as blanket permission without risking a breach of the applicable data protection legislation in either jurisdiction.

3.3.6 Other

Under the Israeli Privacy Law, disclosure to the PCAOB would be allowed where it took place in the ordinary course of business of the Firm and there was going to be no

[18] The United Kingdom Information Commissioner, who enforces the Data Protection Act 1998, may in future take a wider view of "public interest" in light of the definition that will be adopted under the Freedom of Information Act 2002 – however, this is only an informed view.

publication of the data. However, it remains unclear to what extent the delivery by Firms of certain personal data to the PCAOB is in the ordinary course of their business. Furthermore, this exception would not apply where the PCAOB may make available information published which has not been granted confidential treatment.

3.4 Exceptions to the Restrictions on Transborder Data Flow

The following are the relevant exceptions which may apply to legitimise transfer of personal data to the PCAOB in the United States:

3.4.1 Consent

The data subjects give their consent. The EU Data Protection Directive provides that this consent must be unambiguous, which will normally need to be express and in writing. Note that this exception is distinct from the possibility of legitimising disclosure more generally by the use of consent, although the same caveats relating to consent as identified in paragraph 3.3.1 above apply.

3.4.2 Transfer necessary for reasons of public interest

This exception is set out in the EU Data Protection Directive and is therefore relevant for Member States of the EU, although the same caveats apply relating to what will be deemed by each jurisdiction as being in the public interest as identified in paragraph 3.3.2. Furthermore, it is worth noting that this exception is even more restrictive than the exception identified in paragraph 3.3.2 above.

3.4.3 EU Model Clauses

These clauses enable a Firm based in an EU Member State and registered with the PCAOB to agree to transfer the data on the basis of the EU model contractual clauses as approved by the European Commission which, if adhered to by the relevant foreign authority (i.e. the PCAOB), would justify the transfer of personal data to the PCAOB. These would be put in place between Firms and the PCAOB.

3.4.4 Bespoke Contract

The EU Data Protection Directive enables a Firm based in an EU Member State and registered with the PCAOB to agree to transfer the data on the basis of individually drafted contractual clauses which would need to be approved by data protection authorities. The aim of such contracts would be to ensure that the PCAOB has in place adequate data protection procedures to ensure the security of the data transferred. . In addition, if onward pubic disclosure of the personal data in the United States, which has not been granted confidential treatment, is not contractually restricted, the data protection authorities may not approve the contract.

Alternatively, this exception may be fulfilled by the Firms/the European Commission and the PCAOB entering into bilateral/multilateral arrangements. Indeed, the opinion of the Article 29 EU Data Protection Working Committee is for relevant regulators to enter into a dialogue to reach an acceptable compromise. However, a recent resolution of the European Parliament has created doubt as to the validity of this approach[19].

[19] In March 2003, the European Parliament rejected an agreement between the European Commission and United States immigration services in relation to the transfer of passenger records pursuant to the requirements of the United States Aviation and Transportation Security Act 2001. The European Parliament considered this agreement lacked legal basis.

Swiss data protection legislation also provides that a transfer of personal data to the PCAOB may take place if the transferor (the Firm) and the recipient (the PCAOB) of the personal data enter into a contractual agreement whereby the recipient undertakes to follow the requirements of Swiss Data Protection Legislation. For example, such an agreement would have to provide for the duty to keep the personal data confidential. In addition, the Swiss Data Protection Legislation specifically provides that the data may not be disclosed to any other authorities. Furthermore, the data subjects must have knowledge of the data transfer; otherwise the transfer has to be notified to the "Eidgenössischer Datenschutzbeauftragter" ("Federal Data Protection Mandatee").

3.4.5 European Commission finding of "adequacy"

Article 25 of the EU Data Protection Directive mandates the European Commission to determine if data to be transferred to third parties will be protected in an "adequate" fashion. This has not yet been done in respect of data transfers to the PCAOB and, if it were to be considered in the future, the European Parliament would have to decide whether the data protection arrangements in place are adequate. Again, the extent to which the information which has not been granted confidential treatment, can be ring fenced from onward public disclosure in the United States, is likely to be relevant to any assessment of adequacy. Further, this exception applies only to EU Member States and would not assist in the other jurisdictions.

4 Confidentiality

4.1 Client Confidentiality

In all the jurisdictions that we surveyed, the duty of confidentiality between a Firm and its client is very strict. As well as being set out in various laws and regulations in each jurisdiction the requirement of confidentiality may also be implied or expressly set out in the contract or engagement letter each Firm has with its client. These requirements lead to potential conflict with the requirements of the Act relating to the disclosure of client information, in particular pursuant to the PCAOB's ongoing oversight role (see further paragraph 3.1.1 above).

These requirements lead to a potential conflict with those Sections of the Act which: compel registrants to provide the names of certain issuers for which the Firm has prepared or issued audit reports and the annual fees received from such issuers by the Firm[20]; compel registrants to give their consent to co-operate in and comply with all requests for testimony or the production of documents made by the PCAOB[21]; allow the PCAOB (i) to conduct inspections at the registrants in relation to selected audit and review arrangements and (ii) to evaluate the audit, supervisory and quality control procedures of the registrant[22]; and allow the PCAOB to conduct an investigation of any act, practice, or omission to act by a registered Firm[23].

In France, Article L225-240 of the French Commercial Code provides that auditors and their assistants and expert advisers shall be bound by professional secrecy as regards all acts, events and information of which they may have become aware in the course of their duties.

---

[20] Section 102 (b) (2) (A), (B) of the Act

[21] Section 102 (b) (3) of the Act

[22] Section 104 (d) of the Act

[23] Section 105 (c) (1) of the Act

Article 321 of the Swiss Penal Code provides a general secrecy duty on certain professionals including accountants. This will protect all information which the Firms' clients want to keep confidential where it has become known to the Firms in their professional capacity. This provision will be breached regardless of whether the information is revealed orally, for example by giving testimony, in writing or by furnishing the PCAOB with copies of the documents containing the information. Furthermore, the Swiss anti-espionage legislation, which is broadly applied, makes it an offence to make available business information to a foreign authority where it is deemed not to be in the interests of the Swiss Confederation (please see paragraph 8 below for further details).

Likewise, Article 27 of the Japanese Law concerning Certified Public Accountants 1948 prohibits any accountants from disclosing their clients' secrets, which they gained during the course of business, to a third party or making use of them for the accountants or a third party's benefit without due reason. The Code of Ethics established by the Japanese Institute of Certified Accountants provides that accountants will have "due reason" where they have obtained the client's consent or are complying with a legal obligation in Japan.

In Germany, a similar requirement is set out in Section 9 of the Accountants' Professional Articles of Association. Also, Section 323 of the German Commercial Code and Section 43 of the Accountants Ordinance trigger the accountant's duty to keep information confidential. The accountant's duty of confidentiality is far reaching and includes all circumstances the accountant (i) was made aware of by the client and (ii) became aware of during the provision of professional services to a client. To this end, the name of and the amount of fees paid by a client are confidential information. In Germany, in addition to a duty to keep information confidential, an accountant has the right to refuse to testify in civil, criminal and administrative proceedings.

In Mexico, the Law of Professions 1945 provides a general obligation on any person holding a professional qualification, including accountants, to keep "in strict secrecy the matters conferred upon them by clients". In addition, a Code of Ethics of the Mexican Institute of Public Accountants ("**MIPA**") reinforces this requirement via Principle VI which sets out an obligation on accountants to keep confidential all data relating to their client practice.

In the United Kingdom the duty of confidence is reflected in the Institute of Chartered Accountants in England and Wales ("**ICAEW**") Members Handbook. There is a general duty to keep all information confidential, not merely to take all reasonable steps to do so, subject to certain exceptions identified in paragraph 4.4 below. Moreover, it is not just a duty not to communicate the information to a third party, it is a duty not to misuse the information, not to make any use of it or to cause any use of it to be made by others otherwise than for the client's benefit without the consent of the client. This includes a duty not even to disclose the client's name and a duty not to provide an account of facts that could identify any particular client. Confidentiality also extends to third parties from or about whom information has been received in confidence.

4.2 Employee Confidentiality

It is apparent that in some jurisdictions confidentiality obligations will not only arise in relation to the relationship a Firm has with a client but also in an employee context. These requirements lead to a potential conflict with the Sections of the Act which: compel registrants to reveal information relating to criminal, civil, or administrative actions or disciplinary proceedings pending against any associated person of the Firm in connection with any audit report[24]; and compel registrants to give

[24] Section 102 (b) (2) (F) of the Act.

their consent to co-operate in and comply with all requests for testimony or the production of documents made by the PCAOB[25].

In the United Kingdom, the employment relationship gives rise to an implied duty of confidence between the employer and the employee. Information held by an employer, such as details of disciplinary proceedings, may be regarded as confidential to the employee. The disclosure of such confidential information would constitute a breach of confidence and a breach of the implied term of trust and confidence.

Likewise, in Germany as a result of the employer's duty of care, an employer is, as a matter of principle, obligated to keep personal data confidential in order to safeguard the personal rights of an employee. Therefore, the disclosure of personal data, such as the employee's salary or other relevant employee data required by the PCAOB, could violate the personal rights of an employee.

4.3 Sanctions

There are various sanctions that may be imposed where this duty of confidentiality is breached. It is clear that in many jurisdictions a natural person acting on behalf of a Firm is punishable personally. In Japan, for example, an individual accountant who is in breach of this obligation may be imprisoned or fined JPY 1 million. In Switzerland, breach of the requirements under Article 321 of the Penal Code is punishable by up to three years imprisonment or a fine and, in addition, the Firm may be liable for damages in certain circumstances. In Germany, any illegitimate disclosure by an accountant of a client's confidential information is a criminal offence pursuant to Section 203 of the German Penal Code (Strafgesetzbuch) and Section 333 of the German Commercial Code and is subject to fines and imprisonment of two years maximum. In addition, a breach of Principle VI of the Code of Ethics in Mexico could technically lead to the expulsion of that Firm from MIPA.

The breach of professional secrecy by a French auditor is a criminal offence sanctioned by imprisonment of up to one year and a fine of up to € 15,000[26]. In addition to criminal sanctions, the breach of professional secrecy by a French auditor would lead to disciplinary sanctions and possible civil liabilities. Most importantly, the prior consent of a client for the disclosure of information may prevent the auditor from potential civil liabilities vis-à-vis such client, but would not release the auditor from criminal and disciplinary sanctions, as professional secrecy is deemed a core and essential obligation of the profession and is required by law. In Germany, Section 203 of the Penal Code provides that a certified public accountant who discloses a client secret without authorisation may be imprisoned for up to one year or fined up to €1,800,000. Furthermore, in accordance with the German Accountants Ordinance they may be excluded from the profession.

Where there has been a breach of the obligations of confidentiality to an employee in the United Kingdom or Germany an employee could seek an injunction from the courts to prevent the disclosure of such confidential information. In the United Kingdom, the disclosure of information to the PCAOB in breach of an injunction would constitute contempt of court, the penalty for which is a fine and/or imprisonment.

4.4 Exceptions

4.4.1 Consent

[25] Section 102 (b) (3) (A) of the Act.

[26] Article L226-13 of the French Penal Code)

In most of the jurisdictions surveyed, obtaining client consent to disclosure of confidential information would permit the disclosure of information to the PCAOB. However, the same caveats apply as set out above in paragraph 3.3 and the limitations on consent in France should be noted (see paragraph 4.3 above).

In Mexico, for example, there would be no breach of Mexican law where an authorised officer of the client provided the Firm with an acknowledgement that (i) it is an issuer reporting to the SEC; (ii) that it is subject to reporting obligations to the PCAOB pursuant to the Act; and (iii) that it will require its external auditors to register with, comply with the requirements of and report to the PCAOB in accordance with the Act.

It is worth noting that, in the United Kingdom at least, obtaining the consent of an employee to overcome the issues of confidentiality will not override the privilege against self- incrimination (see paragraph 5 below).

In Switzerland, prior consent of a client would not release a Firm from criminal liability where they are in breach of the anti-espionage legislation, which is broadly applied, making it an offence to make available business information to a foreign authority where it is deemed not to be in the interests of the Swiss Confederation (please see paragragh 8 below).

Finally, where banking secrecy obligations apply (please refer to paragraph 6 below) the consent of both the bank and third parties (i.e. the clients of the bank) whose information is also disclosed would be required. Obtaining such consents will be a huge logistical challenge and may, in some circumstances, be impossible.

4.4.2 Public Interest

In the United Kingdom, paragraph 13 of Statement 1.306 of the ICAEW Members Handbook states that a member is free to disclose information that would otherwise be confidential, where such disclosure is justified in the public interest, although the same caveats apply relating to what will be deemed as being in the public interest as identified in paragraph 3.3.2. The Members Handbook states that, whilst the concept of public interest is recognised by the courts, no definition has ever been given. However, the ICAEW expressly recognises that the public interest exception is narrow and the courts have tended to view the public interest defence very strictly, in that it applies where there is a real need for disclosure, such that the duty of confidentiality would be contrary to public policy.

A distinction may therefore need to be made between disclosures given in respect of *specific* requests by the PCAOB (e.g., in relation to suspected criminal activity) and disclosures given in respect of *general* ongoing requests by the PCAOB (e.g., in relation to annual notification of the names of all the issuers for which the Firm has prepared audit reports). In relation to the former, it is arguable that disclosure is in the public interest. In relation to the latter, we do not believe that disclosure will be in the public interest as only certain categories of data are likely to be relevant to any particular public interest.

4.4.3 Legal Obligation

In some jurisdictions, for example the United Kingdom and Japan, the obligation of confidentiality will not be breached where disclosure is carried out in compliance with a legal obligation.

In the United Kingdom, for example, paragraph 20-21 of Statement 1.306 of the ICAEW Members Handbook permits disclosure if authorised by statute. However, in respect of non-governmental bodies (which the PCAOB would likely be defined as), paragraph 22 states that members should not comply with bodies' requests without client consent.

In addition, in respect of suspected breaches of foreign law, paragraph 78 of Statement 1.302 of the ICAEW Members Handbook states that if a member becomes aware of contraventions by his client of foreign law he is under no duty in English law to disclose the matter to the relevant foreign authority regardless of whether he may be under such a duty in foreign law. In the current context, we would agree.

A disclosure required by statute is therefore likely to be restricted to a local statute and, in the absence of an obligation to disclose information to a United States regulator, would not permit disclosure in this case.

5 Employment Law Liability

5.1 Compliance with requests for testimony

In certain jurisdictions, including the United Kingdom, Germany and Japan, the requirement under the Act for Firms to agree to secure consent from all associated persons regarding compliance with requests for testimony and the production of documents could give rise to employment law liabilities and in particular, liability for unfair dismissal.

In order to obtain such consent, Firms would in practice need to make offers of employment conditional upon this consent being obtained. In the event that a Firm makes it a ground for dismissal to refuse such consent, and an employee is dismissed or leaves his or her employment as a result, it is likely to face employment liability in the United Kingdom[27] and Germany.

However, in the United Kingdom, even if consent is obtained, employees may have the right to refuse to testify or disclose documents on the grounds of the privilege against self-incrimination. Under English law the principle of privilege against self-incrimination provides that a person shall not be coerced by the exercise of state power to convict himself/herself of a crime or expose himself/herself to any criminal penalty. If the PCAOB is an "emanation of the state", any associated person required to disclose information could refuse to disclose such information on the grounds of privilege against self-incrimination if the disclosure would incriminate the individual under English law.

Similarly, in Germany, even if the employees' consent can be obtained, the employer cannot fully rely on such consent. According to mandatory provisions of German law, an employee cannot be required to disclose criminal convictions to the employer, unless the conviction is registered in the Federal Central Register of previous convictions (which only applies for severe crimes) *and* the conviction is relevant for the specific occupation of the employee. Furthermore, in accordance with Section 383 of the German Civil Procedure Act and Section 53 of the Criminal Procedure Act accountants have the right to refuse to testify in administrative proceedings in civil, criminal, tax and administrative proceedings.

[27] In the United Kingdom, for example, the Firm is likely to face employee claims of unfair dismissal.

5.2 Suspension of Employees

In certain territories, the PCAOB's powers under the Act to suspend or bar an individual from being associated with a Firm gives rise to certain employment law issues.

In Germany any notice of termination of employment given by a Firm is void unless such notice is justified under the Protection from Dismissal Act.

Under English law any sanction imposed on an employee must be proportionate to the employee's act or omission. Therefore, if an accounting Firm dismissed an employee following an order from the PCAOB, an employment tribunal could rule that the dismissal was a disproportionate sanction and unfair. In addition, in the United Kingdom, if an employee is dismissed for refusing to disclose documents and is protected by the privilege against self-incrimination, the dismissal will be unreasonable and therefore unfair. The failure to carry out a fair disciplinary procedure can also give rise to a breach of the implied duty of trust and confidence under English law owed by an employer to an employee, leading to damages for breach of contract.

6 Banking Secrecy

6.1 Restrictions

Some of the jurisdictions we surveyed have banking secrecy legislation which requires banks and their officers and employees to keep secret the identity of their clients and the details of their relationship with them. This will be particularly relevant where a Firm has banking clients.

In Switzerland, for example, Article 47 of the Banking Act protects information about the clients of Swiss banks, including their names and the mere fact that a certain person is a client of a bank. This obligation is also set out in the Federal Act on Stock Exchanges and Securities Trading in relation to clients of securities dealers and participants of the stock exchange. Both pieces of legislation will specifically apply to a bank's auditors. Disclosure of information required by the Act would result in a breach of the banking secrecy legislation. There are also obligations in Mexico for auditors of a financial institution. In addition, although not part of the jurisdictions that we surveyed, we are aware that similar legislation exists in Luxembourg and Brazil. The Brazilian constitution establishes in Article No. 5, item XII the concept of banking secrecy, which is further regulated by Law no. 105[28] which applies to the secrecy of transactions carried out by financial institutions.

6.2 Sanctions

A breach of Swiss banking secrecy legislation is a criminal offence punishable by up to six months imprisonment or a fine. Infringement of banking secrecy legislation in Luxembourg is also subject to criminal sanctions and may lead to civil liability and regulatory sanctions. Furthermore, breach of banking secrecy obligations in Brazil may result in criminal liability of up to four years imprisonment.

6.3 Exceptions

In Switzerland and Brazil the consent of the banks and their clients will be required and in Mexico it will be necessary to obtain the consent of the National Banking and Securities Commission. Again, however, similar caveats exist with regard to such consent as set out in paragraph 3.3.1

[28] Enacted on 10 January 2001

above. The process of obtaining the consent of the bank's clients in both Switzerland and Brazil will be a huge logistical challenge and may, in some instances, be impossible.

7 Legal Enforcement Issues

All the jurisdictions surveyed raised issues in relation to the PCAOB conducting inspections of a Firm's operations and practice. These issues relate to restrictions on extraterritorial enforcement of legal obligations and, in some territories (for example, Switzerland), the issues cannot be overcome by consent of the Firm.

In Germany, for example, even if the PCAOB carries out an inspection on German territory with the agreement of the concerned Firm, issues of German sovereignty arise. In principle, foreign governmental authorities have no right to carry out acts of state, such as an inspection of the business of a Firm, on German territory without the permission of the government.

In the United Kingdom, Israel and Japan, if the PCAOB wanted to conduct an inspection of a Firm, it would in practice only be able to do so where the Firm is prepared to cooperate. One would expect such cooperation to be given. However, where the Firm is not prepared to cooperate, an order from a competent United States court to inspect a Firm will not in principle be endorsed by a competent United Kingdom, Japanese or Israeli court. The situation would be different where there existed parallel powers between regulators, but this is not the case here.

In Switzerland, Article 271 of the Penal Code forbids without the approval of the competent authorities, on the Swiss territory, the performance of all acts in favour of a foreign state (or a foreign organisation) that are normally performed by state authorities. In such circumstances, it is highly probable that the PCAOB qualifies as a foreign organisation and that, generally speaking, requests and subpoenas by the PCAOB to produce personnel for questioning or to give testimony, to produce and furnish copies of working papers and to submit other information, as well as inspections of a Firm's operations would constitute acts that are normally performed by state authorities. Indeed, the PCAOB could be viewed as part of the authorities protecting United States investors , a function which, from the Swiss perspective, is in principle a governmental one. Thus, such acts are forbidden under Article 271 of the Penal Code.

Since Article 271 protects Swiss sovereignty, the consent of a private person, including the audit client, cannot exempt those performing obligations on behalf of a foreign state from punishment. This approach is mandatory and cannot be bypassed to allow for direct requests or subpoenas from the PCAOB and the officers of the PCAOB and, possibly the employees of the Firm who respond to such requests, could be subject to imprisonment of between three days and twenty years. However, where a request has been made pursuant to the rules of international judicial assistance or with the authorisation of the competent Swiss authority, the respective Firm may, voluntarily, make the required disclosures to the PCAOB.

In Mexico, similar issues of sovereignty arise and, under the bill of rights section of the Constitution[29] a person cannot be mandated to follow a conduct other than by a "competent authority". For these purposes, a Mexican Court is unlikely to consider the PCAOB to be a competent authority.

[29] Articles 14, 16 and 17

8 Official Secrets

8.1 Restrictions

In the United Kingdom[30] and Germany rules exist to protect national security which prevent unauthorised disclosure of certain information to protect the state from espionage etc. Occasionally, a Firm will have sensitive documentation of relevance to national security in its possession and these restrictions will apply.

Similar restrictions apply in Israel where, under the General Security Service Law 2002, a government agency known as the General Security Service has been established for the purpose of protecting national security and is responsible for the protection of certain sensitive information, as determined by the Israeli Government. The holder of such information is required to handle it in accordance with regulations enacted by the Prime Minister. Again there will be circumstances where a Firm holds information that is subject to these restrictions, for example, where a Firm acts as auditor for defence contractors (and we note that a number of such companies are publicly traded in the United States securities markets), it may well be subject to these restrictions.

The anti-espionage legislation[31] in Switzerland is broadly applied making it an offence to make available business information to a foreign authority where it is deemed not to be in the interests of the Swiss Confederation. Given that these provisions are aimed at protecting the confidentiality of the Swiss Confederation rather than private individuals, prior consent of a client would not release a Firm from criminal liability where they are in breach.

8.2 Sanctions

In the United Kingdom, where a Firm is subject to the Official Secrets Act 1989, a person will be subject to criminal sanctions where he discloses any information, document or other article relating to security or intelligence which is or has been in his possession during the course of his work.

Breach of the Swiss anti-espionage legislation is a criminal offence punishable by three days to twenty years in prison.

[30] The Official Secrets Act 1989

[31] Article 273 of the Penal Code