From
ASSIREVI
Via Vincenzo Monti, 16
20123 Milano
Italy
0039 02 436950
0039 02 8801233

Questions connected the provisions of Italian Data protection regulations with respect to the registration system proposed by PCAOB for public firms

This memorandum discusses the main issues connected with Italian Data Protection regulations with respect to the registration system proposed by the Public Company Accounting Oversight Board ("the Board") for public accounting firms wishing to prepare or issue audit reports on US public companies, or to play a substantial role in the preparation or issuance of such reports.

According to this registration system, the public accounting firms must disclose personal and sensitive information regarding third parties.

In Italy, all personal and sensitive data regarding third parties must be handled pursuant to Law no 675/96 (the "Law"), issued, in line with EU Directive 95/46, to ensure that the processing of personal data is carried out protecting the rights, fundamental freedoms and dignity of natural and juridical persons.

With regard to application for registration, we would like to point out the following issues:

- as per Article 28 of the Law [1], personal and sensitive data regarding third parties can be transferred by the "Controller" (in this case the public accounting firms) to a foreign country only if it guarantees an adequate level of protection of the privacy of the parties involved. In the United States, unlike in Italy and the rest of the European Union, the protection of sensitive data regarding third parties is largely based on self-regulation. For the US, the European Commission therefore issued Decision 2000/520/EC, which establishes the criteria on which "adequate levels of protection" are based. According to the Decision, to reach this level, the data must be transferred to US entities that declare (even through self-certification) that they adhere to the Safe Harbor Privacy Principles, as well as to the FAQs, as published by the United States Department of Commerce on 21 July 2000.

  Therefore, in order to ensure that data transferred to the US are adequately protected, the public accounting firm must, as the Controller of such information, verify whether or not the Board is among those companies that meet such requirements or, in any case, if it possesses the appropriate means to guarantee that the data will be processed according to a protection level that is equal to that provided by Italian laws. Indeed, if damages are claimed by one or more of the data subjects [2], it is up to the public accounting firm to provide evidence that it acted with the utmost diligence and that it did everything in its power to avoid the offence.

  Appraisals of the adequacy of the level of protection provided by the destination country are subject to evaluation by the Italian supervisory authority ("Garante") to which, pursuant to Article 28 of the Law, the public accounting firm must give notice **in advance** of its intentions to transfer personal and judicial information to the United States. Should the Garante deem for whatever reason that the intended method of data processing could compromise the adequacy of the level of data protection, it may prohibit the transfer. It follows that the public accounting firm cannot disclose any information to the Board until it obtains authorization from the Garante. In addition, in order to obtain authorization, the public accounting firm must supply the Garante with detailed information as to the type of

---

[1] According to **Article 28 of the Law,** "The cross-border transfer of personal data undergoing processing, temporarily or not, in any form and by any means whatsoever, shall have to be notified in advance to the *Garante* if the country of destination is not a Member State of the European Union. Said transfer may be carried out no earlier than fifteen days after the date of notification; the term shall be twenty days where the transfer concerns any of the data as per Articles 22 and 24. The transfer shall be prohibited where the laws of the country of destination or transit do not ensure an adequate level of protection of individuals. Account shall also be taken of the methods used for the data transfer and the proposed processing, of the purposes thereof, the nature of the data and the relevant security measures."

[2] Persons or entities whose data are handled.

data it intends to transfer and the purposes for which the data will be handled. The public accounting firm must therefore be informed beforehand of how the Board will use such data. However, the Board reserves the right to decide whether or not to accept applicants' requests for the confidential treatment of their data only after it has received such data (see PCAOB Release no 2003-1 Appendix 1-Proposed Rules Relating to Registration - Page A1-ix, point c). Under Italian law, this is not possible since the Garante cannot grant authorization unless it is first informed of the use that will be made of the data once they are transferred abroad.

- **Information requirements and consent.** In view of the above, and in compliance with Articles 11, 20 and 28 of the Law, personal data may be transferred from Italy to the United States only if the data subject has expressly given consent. Such consent must be specific and informed (*ie*, the data subject must be aware of the purposes for which the data is being transferred to the US entity) and, where the transfer concerns judicial or sensitive data, must be given in writing. This obligation also applies to public accounting firms when they request the confidential treatment of information by the Board. Therefore, even in this case the data subject would have to be informed before the transfer of the purposes for which the Board intends to use such information. Consequently, the public accounting firm will not be able to disseminate the information until the Board has guaranteed that it will treat the data confidentially. Should the Controller fail to comply with this obligation, it could commit the crime described in Article 35 of the Law, namely the unlawful processing of personal data. Unless the offence is more serious, any person who, with a view to profiting himself or another, or with intent to cause harm to another, discloses personal data without having received prior consent from the data subject, is punishable by imprisonment for between three months and two years. Finally, we wish to point out that, from a practical point of view, though it is possible to inform and obtain the consent of parties with which the public accounting firm, at the moment of its registration application, has dealings (*eg*, current clients and employees), it is unlikely that this would be possible with regard to former employees or clients with whom relations are no longer maintained.

- **Relevant and not excessive use of personal data.** In light of the above, even if all the conditions making the transfer of personal data regarding third parties by the public accounting firm to the US entity are legitimately met, the data must still be transferred in compliance with Article 9 (1) (d) of the Law. This provision states that personal data undergoing processing must be " relevant, complete and not excessive in relation to the purposes for which they are collected or subsequently processed". Thus, in the case in hand, it would be necessary to make sure that the data, requested by the Board from the applying public accounting firm, is legitimate and not excessive to the purposes for which the request was made (*eg*, requests regarding various judicial information on any data subject that is in any way linked to the public accounting firm).

To summarize:

1) to transfer personal data to the US, the entity to which the data is sent must adhere to the Safe Harbour Privacy Principles or show that it provides a protection level that is equal to that provided by Italian laws;

2) the public accounting firms can not communicate data to the Board without prior guarantee that such data shall be treated confidentially;

3) to transfer "standard" personal data (*eg*, name, address), the data subject's consent must be informed, express and specific;

4) in transferring judicial data (criminal records and current charges), the data subject's consent must not only be informed, express and specific, but must also be in writing.

We remain at your disposal for any further clarifications or information you may need.

Yours faithfully