THE MALTA INSTITUTE OF ACCOUNTANTS

Technical Department
November 2011

Guidance Notes

Data Protection Issues arising from the Transfer of Audit Working Papers to Other Jurisdictions

TECH 01/11

These Guidance Notes are issued by the Malta Institute of Accountants, in November 2011 to identify data protection issues which auditors should consider prior to transferring audit working papers to group auditors in other jurisdictions, as required by the Companies Act, the Accountancy Profession Regulations, 2010 and the International Standard on Auditing (ISA) 600. They also identify various issues arising from legal and other considerations, and aspects dealing with different regulatory procedures in other countries.

These Guidance Notes are intended to provide practical guidance to Members and are not, and should not be interpreted as, a substitute to any legislation, ISA, or parts thereof. These Guidance Notes should be read in conjunction with the relevant legislation, directives and standards. The Malta Institute of Accountants shall not be responsible for any loss sustained by any person who relies on these Guidance Notes.

Contents | **Paragraph Numbers**

These Guidance Notes have been endorsed by the Office of the Information and Data Protection Commissioner on 14 November 2011.

Preface

(a) Legal and professional requirements on transferring audit working papers might vary in terms of the Accountancy Profession Regulations, 2010, ISA 600, the Data Protection Act and the Companies Act.

(b) Article 10 of the Accountancy Profession Regulations, 2010 (hereinafter referred to as "APR") deals with the responsibility and obligations borne by group auditors in the preparation of audit reports on consolidated financial statements.

(c) Paragraph 3 of the ISA 600 refers to the fact that a group auditor may decide to use the audit evidence on which the audit opinion of the financial statements of a component[1] is based to provide audit evidence for the group audit. There may be factors which affect the group auditor's decision as to whether using an audit required by statute or regulation, or opting to provide audit evidence for the group audit. Factors may include differences in financial reporting framework applied in the preparation of the component's financial statements, differences in auditing and other standards applied by the component and the group auditor, and factors such as whether the audit of the component's financial statements will be completed in time to meet the group reporting schedule.

(d) Auditors might be requested to transfer audit working papers compiled during the audit of one or more subsidiaries to the auditors who are expressing an audit opinion on the consolidated financial statements. Auditors need to be aware of their obligations under the Data Protection Act (hereinafter referred to as "DPA") when it comes to transferring audit working papers to a foreign jurisdiction for group audit reporting purposes. For instance, the auditor needs to identify whether he / she is a data controller or a data processor.

(e) A controller of personal data is a person who alone, or jointly with others, determines the purposes and the means of the processing of personal data. The data controller has to abide with a number of obligations, and ensure that the processing is, amongst other criteria, carried out at a level of security appropriate to the nature of the particular personal data and in such a way that the rights of data subjects (natural persons to whom the personal data relates) are protected. Furthermore, the controller has the obligation to notify the Commissioner of Data Protection about the processing.

(f) In all services governed by statute (including statutory audit in terms of the Companies Act), the auditor is the data controller as he / she alone determines the means and purposes for the processing of data. The auditor, for instance, will decide what detailed procedures to perform, what information to collect in order to carry out those procedures, how to store the information collected and how to process it.

(g) On the other hand, a data processor is a person who processes personal data on behalf of the controller and acts on the instructions of the data controller. The obligation of notification to the Commissioner of Data Protection is not assumed by the data processor.

[1] An entity or business activity for which group or component management prepares financial information that should be included in the group financial statements.

(h) The DPA provides for the protection of individuals against the violation of their privacy rights by the processing of personal data. It also deals, amongst others, with the transfer of personal data to other jurisdictions. A transfer of personal data to another country constitutes processing and as such must be notified to the Data Protection Commissioner in the same way as other processing operations.

(i) All processing operations (both manual and automated) by a data controller, and by any person or organisation processing personal data are to be notified to the Data Protection Commissioner in terms of Article 29 of the DPA.[2] The purpose of notification is to register the processing operations. Any new processes introduced by the controller or changes in existing processes should be notified accordingly.

(j) The purpose of these Guidance Notes is to assist auditors in identifying any data protection issues that may arise when a subsidiary auditor is requested to transfer audit working papers to the auditor of the parent company situated in another jurisdiction. The implications differ depending on whether one is transferring audit working papers to EU, EEA, countries recognised by EC and other jurisdictions. (Refer to paragraph 16.)

(k) Article 9 of the APR, dealing with cooperation with competent authorities from third countries, is beyond the scope of this Technical Pronouncement.

[2] Notification may be filed online or else by downloading the Notification Form and sending it by post together with payment, if applicable. A Guide to completing the Notification Form is also available on the website of the Office of the Information and Data Protection Commissioner.

Introduction

1. According to Article 10 of the APR, a group auditor bears full responsibility for the audit report of consolidated financial statements. The group auditor is required to carry out a review of audit work performed by other auditors and maintain related documentation. Moreover, ISA 600 requires the group engagement partner[3] to determine whether sufficient appropriate audit evidence can reasonably be expected to be obtained in relation to the consolidation process and the financial information of the components on which to base the group audit opinion. Access to information is to be available at all times, unless it is restricted by certain circumstances. The Companies Act also refers to the importance of company auditors having right of access to accounting records and other related documentation at all times.

2. As data controllers, auditors need to ensure that personal data is processed fairly and lawfully and always in accordance with good practice. Personal data must only be collected for specific, explicitly stated and legitimate purposes, and must not be processed for any purpose that is incompatible with, inadequate and irrelevant for audit purposes. No further data should be processed than is necessary for the purposes of the audit. Auditors need to make sure that all reasonable measures are taken to complete, correct, block or erase data to the extent that such data is incomplete or incorrect, and that it is not to be kept for periods longer than necessary, having regard to the purposes for which it is processed.[4]

3. The DPA defines personal data as any information relating to an identified or identifiable natural person, who can be directly or indirectly identified, in particular by reference to an identification number or to one or more factors specific to his / her physical, physiological, mental, economic, cultural or social identity. Personal data is treated as sensitive personal data when such data reveals race or ethnic origin, political opinions, religious or philosophical beliefs, membership of a trade union, health or sex life.

4. Audit working papers may include the following information which would fall under the DPA's definition of personal data:
   - payroll data, including leave and sick leave records on payslips,
   - details of individual customers in sales, and / or other accounting records (including credit terms and defaulting clients),
   - details relating to staff members and members of any club, association or other organisation that may be included in a comprehensive list of suppliers and related transactions,
   - shareholders' details, more specifically details about ultimate beneficial owners,
   - directors' remunerations and non-monetary benefits such as medical care, and
   - client acceptance and continuous due diligence documentation.

5. Any person, company, partnership or organisation that processes, stores and uses data of a personal nature in connection with an economic activity has to register under Part VII (Notification and Other Procedures) of the DPA. This also applies to auditors carrying out statutory audits. Auditors need also to refer to Articles 27 and 28 of the DPA before transferring audit working papers to a foreign jurisdiction for group audit reporting purposes. Article 27

[3] The partner or other person in the firm who is responsible for the group audit engagement and its performance, and for the auditor's report on the group financial statements that is issued on behalf of the firm.
[4] Article 7, Data Protection Act (Chapter 440 of the Laws of Malta)

regulates the transfer of data to third countries, that is, countries other than EU Member States, EEA members and other countries which are deemed by the EU Commission to have an adequate level of data protection. Exemptions from the prohibition of the transfer of data to third countries are covered by Article 28.

6. The purpose of these Guidance Notes is to assist auditors in identifying any data protection issues that may arise when a subsidiary auditor is requested to transfer audit working papers to the auditor of the parent company situated in another jurisdiction.

Transfer of Audit Working Papers – Relevant Considerations

Consolidated Accounts of a Group of Undertakings - The Accountancy Profession Regulations, 2010

7. According to Article 10 of the APR, a group auditor bears the full responsibility for the audit report of consolidated accounts, and is required to carry out a review of audit work performed by other auditors, audit entities or firms and to keep related documentation. When a component is audited by third-county auditors or third-country audit entities that have no working arrangement in place, the group auditor may also agree with them to have proper and unrestricted access upon request.

ISA 600 - Special Considerations - Audits of Group Financial Statements (including the work of component auditors)

8. ISA 600 contains requirements for the group engagement partner to have access, when considered necessary, to relevant audit documentation of auditors of significant components in order to obtain sufficient appropriate audit evidence regarding identified and assessed risks of material misstatement affecting the group financial statements.

9. The group engagement partner is responsible for the direction, supervision and performance of the group audit engagement in compliance with professional standards and applicable legal and regulatory requirements. The group engagement partner is also responsible as to whether the auditor's report that is issued is appropriate in the circumstances.[5]

10. The group engagement team shall communicate its requirements to the component auditor on a timely basis. This communication shall set out the work to be performed, the use to be made of that work, and the form and content of the component auditor's communication with the group engagement team.

11. In cooperating with the group engagement team, the component auditor, for instance, would provide the group engagement team with access to relevant audit documentation.[6]

12. The component auditor will also be requested to communicate matters relevant for group reporting purposes, such as:

[5] Para. 11, ISA 600
[6] vide Para. A59, ISA 600

- whether the component auditor has complied with ethical requirements that are relevant to the group audit, including independence and professional competence;
- whether the component auditor has complied with the group engagement team's requirements;
- identification of the financial information of the component on which the component auditor is reporting;
- information on instances of non-compliance with laws or regulations that could give rise to a material misstatement of the group financial statements;
- a list of uncorrected misstatements (above the threshold as set out by the group engagement team) of the financial information of the component;
- indicators of possible management bias;
- description of any identified significant deficiencies in internal control at the component level;
- other significant matters that the component auditor communicated or expects to communicate to those charged with governance of the component entity, including fraud or suspected fraud involving the component entity's management, employees who have significant roles in internal control at the component level or others where the fraud resulted in a material misstatement of the financial information of the component;
- any other matters that may be relevant to the group audit, or that the component auditor wishes to draw to the attention of the group engagement team, including exceptions notes in the written representation that the component auditor requested from component management; and
- the component auditor's overall findings, conclusions or opinion.[7]

13. Where the group engagement team is carrying out the engagement and concludes that sufficient appropriate audit evidence on which to base the group audit opinion is not obtained, it may request the component auditor to perform additional procedures. If it is not possible for the component auditor to perform additional procedures, the group engagement team may perform its own procedures on the financial information of the component.[8]

14. Where the group engagement partner requests access in order to comply with the requirements of ISA 600, the component auditor is presumed to be aware that the group engagement partner intends to use the information in connection with the audit of the group financial statements. A refusal to provide access or to respond to group audit instructions denotes that the group auditor cannot rely on the components auditor's work.

Transferring data to other jurisdictions – Issues emerging from the Data Protection Act [9]

15. Article 29 of the DPA states that a data controller, and any person or organisation processing personal data is obliged to notify the Data Protection Commissioner before carrying out any processing operations.

[7] Para. 41, ISA 600
[8] Para. 44, ISA 600
[9] Articles 27 – 28, Data Protection Act and Legal Notice 155 of 2003 – Third Country (Data Protection Act) Regulations, 2003

16. A transfer of personal data to another country constitutes processing and thus must be notified to the Commissioner in the same way as other processing operations. This applies also when such personal data is to be transferred for group audit reporting purposes. Other than, the obligation of registration with the Commissioner of Data Protection, no restriction or other formality is required when transferring audit working papers containing personal data to group auditors situated in:
    - other EU Member States;
    - EEA[10] members;
    - other countries recognised by the EU Commission to have an adequate level of data protection. The approved list as at preparation time of these guidance notes includes Andorra, Argentina, Australia, Canada, Switzerland, Faroe Islands, Guernsey, State of Israel, Isle of Man and Jersey; and
    - organisations complying with the US Department of Commerce's Safe Harbour Privacy Principles (see paragraph 17), and the transfer of Air Passenger Name Record to the United States' Bureau of Customs and Border Protection. [11]

17. European Parliament and Council Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, prohibits the transfer of personal data to non-European Union (non-EU) countries that do not meet the EU's "adequacy" standard for privacy protection. While both the United States (US) and the EU share the same goal of enhancing privacy protection for their citizens, the US takes a different approach to privacy from that taken by the EU. Consequently, the US Department of Commerce in consultation with the European Commission developed a "Safe Harbour" framework providing various benefits to US and EU organisations:
    a. All 27 EU Member States will be bound by the European Commission's finding of adequacy;
    b. Organisations participating in the US-EU Safe Harbour program will be deemed adequate and data flows to those organisations will continue;
    c. It eliminates the need for prior approval of data transfers, or makes approval from EU Member States automatically granted;
    d. Claims brought by EU citizens against US organisations will be heard in the US, subject to limited exceptions.
    e. It offers a simpler and cheaper means of complying with the adequacy requirements of EU law.

    A full list of organisations which are deemed to have an adequate level of protection is available at http://safeharbor.export.gov/list.aspx.

18. According to Article 27 of the DPA, the transfer of data to a third country is only allowed if there is adequate level of protection. The auditor is required to notify the Data Protection Commissioner of his / her intention to transfer data to a third country.

19. To determine the adequacy level, the Data Protection Commissioner will consider all circumstances surrounding the data transfer operation(s). Attention will be given to the nature of the data concerned, the purpose and duration of the proposed processing operation(s), the country

[10] European Economic Area
[11] The full list of the European Commission's decisions on the adequacy of the protection of personal data in third countries is accessible on http://ec.europa.eu/justice/policies/privacy/thridcountries/index_en.htm.

of origin and country of final destination, the rules of law in force in that third country, and the professional rules and security measures which are complied with in that country.

20. The Commissioner must be satisfied that the data controller has provided adequate safeguards, particularly by the use of appropriate contractual provisions[12]. The use of such provisions is recommended in order to ensure that the rights of individuals are safeguarded in countries which do not ensure an adequate level of protection.

21. As per Article 28(2) of the DPA, a transfer of personal data to a third country that does not ensure an adequate level of protection may still take place, for instance, if consent is given by the data subject. International audit network firms, for example, might have an empowering clause in each contract of employment authorising them to share information with firms of the same network.

22. Even though the Commissioner's approval is not required in such circumstances, the transfer of personal data to third countries is to be notified to the Commissioner as a new process or amendment, unless it had already been notified. There is a special requirement which necessitates the submission of a particular form, known as the International Data Transfer form, downloadable from the website of the Office of the Information and Data Protection Commissioner. In analysing the data transfer, the Commissioner may request from the data controller any relevant information which he deems necessary, in order to verify that the necessary criteria to transfer such personal data are being adhered to.

Right to Information - Requirements under the Companies Act [13]

23. A company's auditor must have a right of access to the company's accounting records and other documentation at all times. The auditor is also entitled to require such information and explanations which are deemed necessary for the performance of his / her duties. Information and explanations may also be asked by auditors to the company's officers when carrying out audit work.

24. The Companies Act makes further reference to the transfer of documents between subsidiaries and parent companies.

25. The officers and auditors of a Maltese subsidiary are required to provide all information and explanations which may be required by the parent company's auditors to be able to carry out the audit of the parent company established in a foreign jurisdiction. If any officer or auditor fails to supply such information, a penalty will be due. Hence, in this case, there are no barriers arising from the provisions of the Companies Act in relation to the transfer of audit working papers.

26. On the other hand, a parent company registered in Malta is required to take all necessary steps to obtain information and explanations from a subsidiary company not registered in Malta. This is only required if requested by the group auditors. If this is not complied with, every officer of the parent company who is in default will be liable to a penalty.

[12] Article 28(3) of the DPA. Click here for further information about model contracts for the transfer of personal data to third countries.
[13] Article 154, Companies Act (Chapter 386 of the Laws of Malta)

27. Nevertheless, the above scenarios do not deal with instances whereby information or explanations are restricted by foreign management or by legislative provisions.

Other Considerations

28. Where a data controller subcontracts business or operational activities and for such reason entrusts a processor with the use of personal data, the controller shall still remain responsible in terms of data protection with regard to such processes carried out on his / her behalf. In these cases, the relationship between the data controller and the data processor shall be regulated by a written contract in accordance with Article 25 of the DPA. In order to facilitate data controllers in complying with the above provision, the Commissioner of Data Protection has developed specific sample clauses which could serve as a basis for developing similar agreements or which may form part of business / service level agreements developed between the parties.[14]

29. Extraterritorial liability issues may arise when transferring audit working papers to other jurisdictions. There is no definite answer as to the applicable law which would apply in such scenarios. It would largely be very much dependant on the type of claim that can be brought, the circumstances in which a claim is brought, and also the specific national legislation of the place of residence of the group auditor. Auditors might wish to seek legal advice in that regard before transferring audit working papers to other jurisdictions.

30. There may also be instances where law or regulation prohibits access to relevant parts of the audit documentation of the component auditor. The group engagement team may request the component auditor to overcome this by preparing a memorandum that covers the relevant information.[15]

31. Another solution would be anonymising data, which effectively stops the data from being personal and therefore removes the restrictions of the DPA. Anonymisation of data consists of amending the data by removing or replacing parts of the data such that the individuals cannot be identified. This process may be needed for ethical reasons to protect people's identities, for legal reasons to not disclose personal data, and also for commercial reasons. This can also be applied when the data subject does not give specific consent for the transfer of personal data or where the Data Protection Commissioner determines that the level of data protection in a particular third country is not adequate. Data may be anonymised by removing direct identifiers (such as name and address), aggregating or reducing the precision of information or a variable (for instance, replacing date of birth by age groups), restricting the upper or lower ranges of a variable to hide those who stand out among others of its kind (in the case of salaries for example), and using pseudonyms.

Conclusion

32. The process of transferring audit working papers to other countries may not always be straightforward. Auditors may consider seeking legal and professional advice when encountering similar scenarios mentioned in previous sections and when having doubt about the applicability of the various provisions of the Companies Act, DPA, APR and ISA 600.

[14] A sample agreement is available on http://idpc.gov.mt/dbfile.aspx/agreementdcprocessor.pdf
[15] Para. A41, ISA 600