the Malta Institute of Accountants

Technical Department
October 2005

Guidance Notes

Practice Guide in Data Protection

For Accountants and Auditors

The Data Protection Act 2001 (Chapter 440)

TECH 03/05

These brief and general guidelines ('the Guidelines') were prepared on the initiative of the Malta Institute of Accountants and have been agreed with the Data Protection Commissioner who, in terms of article 40(g) of the Data Protection Act, has the function to encourage the drawing up of suitable codes of conduct for the various sectors affected by the provisions of the Act. The guidelines are intended to provide practitioners with agreed practices in processing personal data for the different services they offer.

A 'Practitioner's DPA Matrix' is herewith attached to serve as an overview of the principal matters established herein.

Contents (cont.)

Making decisions relating to Data Protection is a complex matter and requires an intimate knowledge of the law and the particular facts to which such law applies. Readers are solicited to obtain tailor-made advice from the Office of the Data Protection Commissioner or from experienced professionals prior to taking their business, strategic, risk management and policy decisions. The Malta Institute of Accountants and all members contributing to the compilation of these guidelines ('the Authors') shall not be responsible for the completeness, and accuracy of the Guidelines. The Authors are not responsible for any damages which may arise from or be connected with the use of the Guidelines. This disclaimer shall be construed as being a part of the Guidelines. The Guidelines reflect information current as in October 2005

Introduction

Legislative History

1. Data protection in Malta is currently regulated by the Data Protection Act, Chapter 440 of the Laws of Malta ("DPA"), which was introduced by Act XXVI of 2001, amended by Act XXXI of 2002 and fully brought into force on 15 July 2003.

2. The following subsidiary legislation has been issued under the DPA:

   Legal Notice (L.N.) 16 of 2003, Processing of Personal Data (Telecommunications Sector) Regulations as amended by L.N.153 of 2003, L.N. 522 of 2004, and L.N.109 of 2005;

   L.N. 154 of 2003, Notification and Fees (Data Protection Act) Regulations, 2003 as amended by L.N.162 of 2004 which has introduced substantially reduced notification fees and exempted certain classes of persons from payment. This regulation exempts from the notification obligation a company where the only personal data processed is that contained in the Memorandum and Articles of Association;

   L.N. 155 of 2003, Third Country (Data Protection Act) Regulations, 2003;

   L.N. 125 of 2004, Processing of Personal Data (Protection of Minors) Regulations, 2004;

   L.N. 142 of 2004, Data Protection (Processing of Personal Data in the Police Sector) Regulations, 2004.

3. Any person or organisation processing personal data is obliged to **comply** with the requirements of the DPA.

Transitory Provisions

4. Electronic processing of personal data initiated prior to the 15th of July, 2003 were required to comply with the provisions of articles 7 to 9 and 12 to 17 of the DPA by the **15th April, 2004.**

5. Manual processing of personal data initiated prior to the 15th of July, 2003 must comply with the provisions of article 7 to 9 and 12 to 17 of the DPA by the **24th of October, 2007.**

6. Some provisions, including those relating to direct marketing, right of access and transfers abroad came into force on **15 July 2003.**

Terminology

7. **Practitioner**: In this document the term has been used to refer to accountants, auditors and to firms of accountants in public practice.

   Least Privilege: To allocate only the minimum level of access rights to data (e.g. read, write, delete, archive, etc) which would allow that person to fulfil his responsibilities.

   Need to Know: To allow a person to only access that specific data which is required for him to fulfil his responsibilities.

Scope of the DPA

8. The primary objective of the DPA is to protect individuals against the violation of their privacy through the processing of personal data. For such purposes the collection, use and distribution of personal data is regulated under the DPA.

9. The DPA applies to the processing of data which takes place in the Maltese territory and where the controller is considered to be established in Malta for the purposes of the DPA.

10. When dealing with data protection issues the practitioner must also take into consideration the obligations arising under other binding statutes or legislative instruments such as the Prevention of Money Laundering Act and the Professional Secrecy Act.

Persons Protected

11. The DPA protects data which refers to individuals as natural persons ("data subject") as opposed to data referring to bodies corporate or legal entities.

Protected Data

12. As the DPA applies to personal data, the processing of any information which is not personal data, is not regulated by the DPA unless such information relates to legal persons in cases of unsolicited communications for the purposes of direct marketing by means of an automated calling machine, fax or e-mail (Regulation 10 of L.N. 16 refers).

13. ***Personal Data*** is broadly defined in the DPA as "any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity."

    It must be appreciated that on account of the fact that the term is broadly defined it will generally include any information held about identifiable individuals.

14. The DPA further defines ***sensitive personal data*** as any "…personal data that reveals race or ethnic origin, political opinions, religious or philosophical beliefs, membership of a trade union, health or sex life;"

    On account of its particular nature *sensitive personal data* is regulated more rigorously than non-sensitive or ordinary personal data. In general the DPA stipulates that sensitive personal data cannot be processed unless the following conditions are satisfied:

    - Specific consent of the data subject has been obtained; or
    - Data has already been made public by the data subject; or
    - Processing is necessary to comply with laws regulating employment; or
    - Processing is necessary to protect the vital interests of data subject who is physically or legally incapable of giving his consent; or
    - Processing is carried out by a Health Professional in the best interests of the patient; or
    - So that legal claims can be established, exercised or defended.

15. Practitioners are to ensure that they adopt the 'need to know' and 'least privilege' concepts when processing personal data and only process as much data as is required to satisfy legislative requirements and accountancy standards.

What constitutes the processing of personal data for the purposes of the DPA?

16. The *processing* of personal data is very broadly defined by the DPA in an attempt to bring any operations or activities, which include personal data within its purview.

17. In fact, any operation (or set of operations) undertaken in regard to personal data, and including the collection, recording, organisation, storage, adaptation, alteration, retrieval, gathering, use, disclosure by transmission, dissemination or even making information available, alignment or combination, blocking, erasure or destruction of such data falls within the scope of, and is regulated by, the DPA.

Obligations of the Data Controller

18. A data controller is any person including a company, organisation, club or individual, who in any way processes data, and determines the means and purposes for the processing of data, pertaining to a natural person (i.e. a human being) for purposes other than private use.

Requirements for Processing

19. Irrespective of the manner with which the relevant data is collected the data controller is in all cases obliged to follow these 8 key points. In terms of Article 7 of the DPA, every controller of data shall ensure:

    1) That personal data is processed fairly, lawfully and always in accordance with good practice;

    2) That personal data is only collected for specific, explicitly stated and legitimate purposes;

    3) That personal data is not processed for any purpose that is incompatible with that for which the information is collected;

    4) That personal data that is processed is adequate and relevant in relation to the purposes of the processing;

    5) That no more personal data is processed than is necessary having regard to the purposes of the processing;

    6) That personal data that is processed is correct and, if necessary, up to date;

    7) That all reasonable measures are taken to complete, correct, block or erase data to the extent that such data is incomplete or incorrect, having regard to the purposes for which they are processed;

    8) That personal data is not kept for a period longer than is necessary, having regard to the purposes for which they are processed.

Notification

20. All the required information as stipulated in Article 29 must be submitted to the Data Protection Commissioner or to the Personal Data Representative. The relevant fee must be paid, if applicable.

21. As for **automated processing operations** of personal data a transition period up to the 14th of July 2004 was established. This one year period gave data controllers sufficient time to notify their existing processing operations.

22. As for **manual processing operations** of personal data, a transition period up to the 24th of October 2007 was established for data controllers to notify such operations.

23. After 15 July 2003, all processing operations, both manual and automated, shall be notified to the Data Protection Commissioner.

Examples of Data Subjects	
Employees	Practitioners that engage employees would retain information about such employees. The purpose for having this information would be: to process their payroll; to satisfy employment legislation; for administration purposes; for sick leave; and, for performance of contract and where adopted for performance reviews.
Examples of Data Subjects (cont.)	
Clients and Suppliers	Irrespective whether the practitioner is exercising his profession via a large audit firm or as a sole practitioner, it is necessary to process information about clients and suppliers of services and products. Even if all clients and suppliers are corporate bodies, in all probability personal data is being processed about officers of those organisations. The purposes for processing these data would mainly be: performance of contract; administration and accounting; legal and regulatory obligations; marketing (possibly); and, legitimate interests arising.

Security Measures

24. Controllers must implement cost-effective and adequate technical and organisational measures to ensure that data is protected against unauthorised access and use, destruction, loss and modification (Article 26). The more sensitive the data the more stringent the controls that need to be applied.

The Role of the Practitioner

25. In the practice of their profession, practitioners have to identify what personal data they process and then determine whether in relation to such data they are the controllers or simply act as processors.

26. Where the practitioner is not a data controller, he is not required to obtain the consent of the data subject and if there is the obligation of consent then this must be obtained by the data controller. In the accountancy profession, where the practitioner processes data in relation to which his client is the data controller, the practitioner does not need to obtain consent where it would be required. It is the client, as a data controller, who should obtain consent in these cases.

Service Lines

27. When examining a practitioner's activities in terms of the DPA, it is important to first establish the underlying framework within which the work is performed. If the practitioner's work is mandated by statute (eg. Companies Act, Cooperatives Act, relevant Acts establishing Government Corporations, such as Enemalta Act, etc) then the performance of that work does

not require the express prior consent of the individual data subjects whose data will be processed as part of the performance of the required statutory work. Such data subjects could comprise *inter alia* clients, suppliers and employees of the entity with regard to which the statutory work is required.

28. Another important issue from the DPA perspective, as stated earlier, relates to whether, when performing a service, the practitioner is a Data Controller or a Data Processor. It is important to identify the role envisaged under the DPA in respect of the performance of services in view of the subject's right of access. If the practitioner is deemed to be the Data Controller then a data subject has the right to request the practitioner for information that is being processed about him unless the practitioner is barred from granting the right of access in terms of professional secrecy. In such cases requests could be made *inter alia* by clients, suppliers and employees of the entity in relation to which the practitioner's work is being performed.

29. Such requests for information need to be considered in the light of professional ethics and standards and relevant legislation which require practitioners to maintain the confidentiality of all information obtained in the exercise of their professional work.

30. Another significant issue relates to the processing of sensitive data of clients' employees without first obtaining the employees' specific consent.

31. Therefore, it is necessary to identify each service line and establish whether the work is mandated by statute and whether the practitioner is acting as a controller or as a processor.

Statutory Work

32. In all the services that are governed by statute (e.g. statutory audit in terms of the Companies Act and audits of public corporations required by the relevant incorporating legislation) the auditor is the data controller as he alone determines the means and purposes for the processing of data. The practitioner 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. The relevant entity and its officers are obliged to provide all the information requested and cannot interfere with the work of the practitioner. In this way, the practitioner's independence from the entity is maintained at all times. The practitioner is at all times bound by professional ethics and standards and by relevant legislation to protect the confidentiality of the data processed.

33. In the case of statutory work, prior consent from individuals on whom information is processed (data subjects) is not required to be obtained, and this on the strength of articles 9(c) and 9(f) of the DPA which state "processing is necessary for compliance with a ***legal obligation*** to which the controller is subject" and "processing is necessary for a purpose that concerns a ***legitimate interest of the controller*** or of such a third party to whom personal data is provided, except where such interest is overridden by the interest to protect the fundamental rights and freedoms of the data subject and in particular the right to privacy".

34. It is to be pointed out that statutory work comprises all work required by statute from a certified public accountant, whether or not this relates specifically to auditing or to the issue of other forms of assurance reports.

35. In terms of the DPA the practitioner can only process as much personal and/or sensitive personal data as is required for the successful completion of the work required by statute, and the data collected cannot be used for any other purpose.

36. The data collected will be stored by the practitioner in a structure that will *inter alia* satisfy relevant professional standards. Typically this storage will not be such as to readily enable identification of relevant data subjects.

37. Data subjects cannot be granted access to data held in the audit files without due consideration of Professional Secrecy obligations.

38. A necessary element of a proper audit is the access by the practitioner to all relevant information, including personal and sensitive personal data. Typically practitioners require to process sensitive personal data when performing detailed testing of payroll computations. This would entail the processing of data relating to health and trade union membership of client staff. Such processing, to the extent that it is necessary for the specific audit, is inherent to the exercise of the accountancy profession by the practitioner. In the light of all these considerations and subject to proper privacy safeguards, the provisions of the DPA do not prohibit such processing.

Non-Statutory Work

39. In this case, to the extent that it is only the client that is determining the means and the purpose for the processing of the data, the practitioner is deemed to be a processor. Therefore, there are no direct obligations under the DPA for the practitioner. In the capacity of a processor, the practitioner is obliged to:

    - Only process the data in accordance with instructions received from the data controller, and
    - Provide the same level of technical and organisational measures to protect the data that is expected from the data controller.

    Furthermore, the processing is to be governed by a contract or other legally binding instrument in a written or equivalent form.

40. The practitioner can maintain records of the task performed to satisfy international auditing standards and regulatory requirements.

41. The practitioner will not utilise any personal data gathered for any other purpose.

42. The practitioner is at all times bound by Professional Secrecy.

Tax Compliance Work

43. Another service provided by practitioners is to assist clients with tax compliance work.

44. Irrespective of whether clients are bodies corporate or natural persons, the practitioner is deemed to be a processor of data. In the capacity of a processor, as in this case, the practitioner is to act on instructions of, and on behalf of, the client without ever determining the means and purposes for processing of any of the data.

45. The obligations of a processor are described in paragraphs 39 to 42 of these Guidance Notes.

46. As in other cases the data cannot be used for any other purpose and, as is the case with other services, Professional Secrecy laws also apply.

Staff Recruitment Services

47. Practitioners offer Staff Recruitment Services to clients and non-clients. This is usually undertaken either by publishing an advert in the local media or by effecting a search through a database of persons who would have already applied under a previous call and who had consented to have their CV retained by the practitioner for future calls.

48. Where in the selection process, the practitioners make only recommendations to their clients and do not select the successful applicants themselves, then the practitioner is deemed to be a **processor**, acting on behalf of their client. The practitioner cannot utilise this data for any other purpose as the data belongs to the client.

49. It is good practice to advise the applicant, through the letter of acknowledgement, of how the process is being undertaken, e.g. that all the applications are being forwarded to the client, or that the client will receive the CV's of the short-listed candidates.

50. When the practitioner has completed his task and provided the client (prospective employer) with the required service, all the CVs and applications submitted by the applicants are to be forwarded to the client, as the data controller. The client may retain these personal data only for a period deemed necessary for recruitment purposes (e.g. probation period), after which such records must be destroyed. Where however the client intends to keep the records for any future vacancies, data subjects must be informed and their consent obtained accordingly.

51. Where the practitioner intends to maintain on file the CVs of unsuccessful applicants for the purpose of filling any future vacancies, the practitioner shall inform the applicants accordingly and obtain prior consent. In this case the practitioner becomes the data controller and must satisfy all the requirements under the DPA.

Liquidations

52. From time to time practitioners are asked to act as liquidators of companies. In their role as liquidators the practitioner is deemed to be an officer of the company and at all times represents the company. Any action undertaken by the liquidator is carried out on behalf of the company.

53. When a company is in liquidation all actions by or versus a company are exercised against the liquidator in his capacity as a legal and judicial representative of the company.

54. The practitioner is neither a controller nor a processor as the company itself maintains the role of controller and/or processor. However it is the liquidator's duty as representative of the company to ensure that all the data protection principles are adhered to in the liquidation process.

Other Practices

Databases and Records

55. Practitioners should:

- Review current information held for accuracy and to ensure it is up to date;
- Periodically update and tidy up all databases;
- Delete unrequired and unreliable information from databases;

- Include “opt-out” tick boxes on any conventional marketing mailings and in case of electronic mailing after obtaining prior consent in writing;
- Obtain consent for collection and processing where necessary;
- Monitor the use of the information to ensure it is used for the purpose set out.

Security and Access Issues

56. Practitioners should improve, where necessary, security and controls on their networks and at their place of work. Some recommendations:
    - Set up user IDs and passwords to protect systems and databases;
    - Develop and implement security policies, especially email, internet and DPA policies;
    - Change passwords regularly;
    - Provide training on DPA obligations;
    - Appoint a partner/manager responsible for firm compliance;
    - Have in place appropriate security measures both technical and organisational.

Data Subject Access

57. Each practitioner should appoint a contact person who is knowledgeable about the DPA and these agreed practices. Furthermore, practitioners should:
    - Set up a standard procedure to deal with access requests e.g. checklist/logbook; and
    - Record all action taken.

Collecting Personal Data

58. When collecting data about individuals, Article 19, requires that data controllers inform the data subject of:
    - Organisation's name (either its own or agent's) and Address;
    - Purpose/s of processing information;
    - Mandatory and optional fields;
    - Who other than the controller will the data be shared with;
    - His right of access, right to rectify and where applicable the right to erase data;
    - And any other details which would ensure that the processing is fair.

Marketing

59. Practitioners could use client data for cross selling of other services they have to offer and also for selling of conferences, seminars or other similar events.

60. Practitioners can send out marketing information by normal surface mail, however, they must always provide their customers with the option to opt out from receiving further similar correspondence.

61. When direct-marketing communications are made by means of emails, faxes and automated calling machines, the practitioner must ensure that they are only marketing their products or services and only to their clients who have already utilised such services. Sending marketing

communications by the same means to different persons would require practitioners to obtain the prior explicit consent in writing; LN16 of 2003 – Electronic Communications Sector, Regulation 10 refers.

Transfer to third countries

62. The requirements of the DPA in relation to third countries, do not apply to:

- EU Member States;
- EAA members; and
- Other countries recognised by the EU Commission to have an adequate level of data protection currently including Switzerland, Canada, Argentina, Guernsey, Isle of Man, the US Department of Commerce's Safe Harbour Privacy Principles, and the transfer of Air Passenger Name Record to the United States' Bureau of Customs and Border Protection.

63. The transfer of personal data to any country is a processing operation which has to be notified to the Data Protection Commissioner. When a transfer is made to a third country that does not ensure an adequate level of protection, an authorisation by the Commissioner is required.

64. The use of appropriate contractual 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.

65. A transfer of personal data to a third country that does not ensure an adequate level of protection may still be effected under the exemptions as set out in article 28(2) of the DPA.

Attachment 1: Practitioner's DPA Matrix

	Statutory Work	Non-Statutory Work	**Tax Compliance Work**	Staff Recruitment Services		**Liquidations**
			Corporate /Personal Tax	**On behalf of a client**	**Applications retained on database**	
Data Controller or Data Processor? (… determines the purposes and means… art 2)	**Data Controller**	**Data Processor**	**Data Processor**	**Data Processor**	**Data Controller**	Company as represented by Liquidator
Processing permitted under DPA criteria ? Art. 9	**Yes**	N/A	N/A	N/A	**Consent is required**	Normal DP regulations apply
Access to data by subject? Art 21	**No** Professional Secrecy	N/A	N/A	N/A	**Yes**	Normal DP regulations apply
May Sensitive Personal Data be processed? Arts 12 - 16	***Yes***	N/A	N/A	N/A	**Specific consent required**	Normal DP regulations apply