DATA PROTECTION ACT 1998

GUIDANCE NOTE 7 - THE SEVENTH PRINCIPLE

Prepared By: Christopher Lambeth
Corporate Information
Governance Officer
Date of Publication: 20th October 2006
Version: 1.3

Table of Contents

1. Version Control

Version	Date	Notes
1.0		Sent out to DP Contacts for comments
1.1	26th July 2006	Updated following comments received
1.2	16th October 2006	Updated with additional comments
1.3	20th October 2006	Updated

2. Points of contact for this Guidance

Corporate Information Governance Team	
Name	Malkiat Thiarai
Title	Corporate Governance & Information Manager
Telephone	0121 303 1909
Email	malkiat_thiarai@birmingham.gov.uk

Document Author	
Name	Christopher Lambeth
Title	Corporate Information Governance Officer
Telephone	0121 303 4876
Email	christopher_lambeth@birmingham.gov.uk

3. Introduction

3.1 The Seventh Principle States:

"Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data".

The Data Protection Act gives some further guidance on matters, which should be taken into account in deciding whether security measures are "appropriate". These are as follows: -

(i) Taking into account the state of technological development at any time and the cost of implementing any measures, the measures must ensure a level of security appropriate to:

(a) the harm that might result from a breach of security; and

(b) the nature of the data to be protected.

(ii) the data controller must take reasonable steps to ensure the reliability of staff having access to the personal data.

With regard to the technical and organisational measures to be taken by data controllers, the Directive states that such measures should be taken " both at the time of the design of the processing system and at the time of the processing itself, particularly in order to maintain security and thereby to prevent any unauthorised processing." Data controllers are, therefore, encouraged to consider the use of privacy enhancing techniques as part of their obligations under the Seventh Principle.

4. Risk Assessment

4.1 Risk Based Approach

It is clear from (i) above that there can be no standard set of security measures that is required for compliance with the Seventh Principle. The Commissioner's view is that what is appropriate will depend on the circumstances, in particular, on the harm that might result from, for example, an unauthorised disclosure of personal data, which in itself might depend on the nature of the data. The data controller, therefore, needs to adopt a risk-based approach to determining what measures are appropriate. (In fact, the Directive refers to "a level of security appropriate to the risks represented by the processing"). Management and organisational measures are as important as technical ones.

4.2 Standard Techniques

Standard risk assessment and risk management techniques involve identifying potential threats to the system, the vulnerability of the system to those threats and the counter-measures to put in place to reduce and manage the risk. In many cases, a simple consideration of these matters will be sufficient. On the other hand, there are well-established formal methodologies, which will assist any data controller to assess and manage the security risks to the system.

5. Security Controls

5.1 Some of the security controls that the data controller is likely to need to consider are set out below. (This is not a comprehensive list but is illustrative only.)

Security management:

- Does the data controller have a security policy in place setting out management commitment to information security within the organisation?
- Is responsibility for the organisation's security policy clearly placed on a particular person or department?
- Are sufficient resources and facilities made available to enable that responsibility to be fulfilled?

Controlling Access to the Information:

- Is access to the building or room controlled or can anybody walk in?
- Can casual passers-by read information off screens or documents?
- Are passwords known only to authorised people and are the passwords changed regularly?
- Do passwords give access to all levels of the system or only to those personal data with which that employee should be concerned?
- Is there a procedure for cleaning media (such as tapes and disks) before they are reused or are new data merely written over old? In the latter case is there a possibility of the old data reaching somebody who is not authorised to receive it? (eg. as a result of the disposal of redundant equipment).
- Is printed material disposed of securely, for example, by shredding?
- Is there a procedure for authenticating the identity of a person to whom personal data may be disclosed over the telephone prior to the disclosure of the personal data?
- Is there a procedure covering the temporary removal of personal data from the data controller's premises, for example, for staff to work on at home? What security measures are individual members of staff required to take in such circumstances?
- Are responsibilities for security clearly defined between a data processor and its customers?

Ensuring business continuity:

- Are the precautions against burglary, fire or natural disaster adequate?
- Is the system capable of checking that the data are valid and initiating the production of back-up copies? If so, is full use made of these facilities?
- Are back-up copies of all the data stored separately from the live files?

- Is there protection against corruption by viruses or other forms of intrusion?

Staff selection and training:

- Is proper weight given to the discretion and integrity of staff when they are being considered for employment or promotion or for a move to an area where they will have access to personal data?

- Are the staff aware of their responsibilities? Have they been given adequate training and is their knowledge kept up to date?

- Do disciplinary rules and procedures take account of the requirements of the Act? Are these rules enforced?

- Does an employee found to be unreliable have his or her access to personal data withdrawn immediately?

- Are staff made aware that data should only be accessed for business purposes and not for their own private purposes?

Detecting and dealing with breaches of security:

- Do systems keep audit trails so that access to personal data is logged and can be attributed to a particular person?

- Are breaches of security properly investigated and remedied; particularly when damage or distress could be caused to an individual?

6. Processing by a Data Processor

6.1 Processing by a Data Processor on behalf of the Data Controller

The Act introduces express obligations upon data controllers when the processing of personal data is carried out by a data processor on behalf of the data controller. In order to comply with the Seventh Principle the data controller must –

- Choose a data processor providing sufficient guarantees in respect of the technical organisational security measures they take,

- take reasonable steps to ensure compliance with those measures, and

- ensure that the processing by the data processor is carried out under a contract, which is made or evidenced in writing, under which the data processor is to act only on instructions from the data controller. The contract must require the data processor to comply with obligations equivalent to those imposed on the data controller by the seventh principle.

Further advice may be found in BS 7799 and 1S0/IEC Standard 17799.

It is important to note that the Seventh Principle relates to the security of the processing as a whole and the measures to be taken by data controllers to provide security against any breaches of the Act rather than just breaches of security.

7. Advice and Assistance

7.1 The Corporate Information Governance Team

The Corporate Information Governance Team provides advice and assistance on the Data Protection Act 1998 and the Freedom of Information Act 2000 as well as other associated legislation. The Corporate Team can be contacted on 0121 303 4876 or in writing at the following address:

Corporate Information Governance Team
Intelligent Client Function
1st Floor, Lancaster Circus
1 Lancaster Circus
Birmingham
B4 7AB

7.2 Directorate Data Protection Contact Officers

Birmingham City Council has a Data Protection Officer within each individual Directorate in order to provide assistance on data protection issues. If you have any concerns relating specifically to your Directorate please contact your contact officer in the first instance and they will be able to advise you accordingly.

A full list of DP Contact officers is available on In-line.

7.3 The Information Commissioner

The Information Commissioner is the governing body for Data Protection and Freedom of Information and is an independent officer who is appointed by the Queen and reports directly to parliament.

The Information Commissioners duties include:

- Maintaining a register of data controllers
- Distribution of information on legislation
- Promoting compliance with the data protection principles
- Considers complaints about breaches of the principles within the Act
- Prosecutes offenders who contravene the Act

The Commissioner is there to help everyone comply with the Act. If you would like further advice on the Act you can contact the Information Commissioner's office at the address below or you can search their web-site to locate useful information on legislation matters.

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF Tel: 01625 545 745

The information contained within this document is taken from the Information Commissioner's Legal Guidance booklet. For further details on the Act please visit the Information Commissioners web-site at > *www.informationcommissioner.gov.uk*