



DATA PROTECTION ACT 1998

GUIDANCE NOTE 2 – THE DATA PROTECTION PRINCIPLES

Prepared By: Patricia Rowson
Corporate Information
Governance Officer
Date of Publication: 20th October 2006
Version: 1.4

Table of Contents

1. Version Control	3
2. Points of contact for this Guidance	3
3. Introduction	4
4. The Principles of Good Information Handling.....	4
5. Schedule 2 Conditions	7
6. Schedule 3 Conditions	7
7. Schedule 4 Conditions	9
8. Advice and Assistance.....	11

1. Version Control

Version	Date	Notes
1.0		Sent out to DP Contacts for comments
1.1	26 th July 2006	Updated following comments received
1.2	6 th September 2006	Updated with additional comments
1.3	20 th October 2006	Updated
1.4	29 th January 2009	Updated

2. Points of contact for this Guidance

Corporate Information Governance Team

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

Document Author

Name	Patricia Rowson
Title	Corporate Information Governance Officer
Telephone	0121 303 4876
Email	patricia.rowson@birmingham.gov.uk

3. Introduction

3.1 The Data Protection Principles

Please ensure that personal data is processed in a fair and lawful manner.

The Data Protection Act 1998 contains eight principles, sometimes referred to as the principles of 'good information handling'. All Data Controllers are required to comply with these principles when processing personal data about living individuals.

Every instance of processing information has to be capable of withstanding rigorous scrutiny regarding fairness. Was any person from whom the information was obtained deceived or misled?

Was the purpose(s) the information would be used for explained to them?

When considering the Principles it is worth remembering the wide scope of the definition of "processing" in the Act and, in particular, the fact that the term includes "obtaining " and "disclosure" of the data.

4. The Principles of Good Information Handling

1st Principle

Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless –

- a) at least one of the conditions in schedule 2 is met and**
- b) in the case of sensitive personal data, at least one of the conditions in schedule 3 is also met**

Interpretation – Personal data are not to be treated as processed fairly unless the data controller ensures, so far as practicable, that the data subject has, is provided with, or has made available to him at least –

- the identity of the data controller*
- the purpose(s) for which data will be processed*
- any further information necessary*

Lawfulness

*Personal data may be processed without the consent of the data subject where there is a lawful obligation to do so. **For example:** Council Tax is administered under the Local Government Finance Act and the Council Tax (Administration and Enforcement) Regulations 1992 and enables local authorities to process personal data without the consent of the data subject.*

Fairness

Although consent is not required for the administration of Council Tax, there is still an element of fairness placed upon the data controller in order to provide data subjects with details of how their personal data is to be processed.

2nd Principle

Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

Interpretation – Purpose(s) may, in particular, be specified in a notice given in accordance with the fair processing requirements or in a notification.
In deciding whether a disclosure is compatible consideration must be given to the purpose(s) for which the data are to be processed by the person to whom they are disclosed.

3rd Principle

Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

Interpretation - The data processed should only be used for the business operations of the data controller and should be no more than is necessary for the purpose(s) for which the data is collected.

If the Data Controller intends to hold data for future processing activities, they should inform the individual at the time of collection of their personal data. This information should be held for the purposes(s) for which it has been collected and not held for some considerable time before being used, because it may subsequently become out dated and would therefore infringe the next principle.

4th Principle

Personal data shall be accurate and, where necessary, kept up to date.

Interpretation – Provides that this principle will not be contravened even if data are inaccurate where they accurately record information obtained from the data subject or third party in any case where

- the data controller has taken reasonable steps in the circumstances to ensure accuracy, and
- if the data subject has challenged the accuracy of the data, the data indicate this.

5th Principle

Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes

Interpretation - This principle revolves around retention periods of data. This therefore will have a two fold effect, firstly Data Controller will need to devise a system, or have it incorporated into any system, a means of removing those records which are no longer required by either departmental policy or statute.

Secondly, it offers the Data Controller the opportunity to keep his/ her data under review and prevent it becoming so large that it hinders the system i.e. speed or using the disk space.

An important exemption to this principle is that data 'held for historical, statistical or research purposes and not used in such a way that damage or distress is likely to be, caused to any data subject' may be kept indefinitely. Any release of such data should be in an anonymous form anyway

6th Principle

Personal data shall be processed in accordance with the rights of data subjects under this Act.

Interpretation – A Data Controller will contravene this principle only if he

- fails to properly respond to a subject access request
- fails to respond to notices from individuals exercising their rights:
 - to prevent processing likely to cause damage or distress
 - to prevent processing for direct marketing
 - to prevent processing in relation to automatic decision-taking

7th Principle

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.

Interpretation – The measures must ensure a level of security appropriate to the nature of the data and the harm that might result from a breach of security. The data controller must take reasonable steps to ensure the reliability of any employees who have access to personal data.

Further guidance on the seventh principle can be located within Guidance Note 7 - The Seventh Principle.

8th Principle

Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Interpretation – In determining what amounts to an adequate level of protection consideration will be given in particular to the following:

- *Nature of Personal data*
- *Country of Origin of Information*
- *Country of final destination of information*
- *Purposes and period of processing*
- *Law in force in the country in question*
- *International obligations of that country*
- *Enforceable Codes of Conduct or one-off arrangements*
- *Security measures*

5. Schedule 2 Conditions

5.1 Schedule 2 contains 6 conditions that will need to be met before any processing activity can take place. At least one of these conditions will need to be satisfied in order to ensure the processing taking place is compliant with the Act.

5.2 Conditions for processing of any personal data as referred to in Principle 1.

Condition 1. The data subject has given their consent to the processing.

Condition 2. The processing is necessary :-

- a) for the performance of a contract to which the data subject is a party, or
- b) for the taking of steps at the request of the data subject with a view to entering into a contract.

Condition 3. The processing is necessary to comply with any legal obligation to which the data controller is subject, other than an obligation imposed by contract.

Condition 4. The processing is necessary in order to protect the vital interests of the data subject (this can only be used for matters of life and death).

Condition 5. The processing is necessary :-

- a) for the administration of justice,
- b) for the exercise of any functions conferred on any person by or under any enactment,
- c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department, or
- d) for the exercise of any other functions of a public nature exercised in the public interest by any person.

Condition 6. The processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case because of prejudice to the rights and freedoms or legitimate interests of the data subject.

6. Schedule 3 Conditions

6.1 Schedule 3 contains 10 conditions relating to sensitive personal data and at least one of these will need to be satisfied in addition to meeting a Schedule 2 condition. The Act defines categories of sensitive personal data and these are mentioned in Section 6.1 within this guidance document.

Categories of Sensitive Personal Data

- The racial or ethnic origin of the data subject
- Their political opinions
- Their religious beliefs or other beliefs of a similar nature
- Whether they are a member of a trade union
- Their physical or mental health or condition
- Their sexual life
- The commission or alleged commission by them of any offence, or
- Any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or sentence of any court in such proceedings

6.2 Conditions relevant for processing of Sensitive personal data as referred to in Principle 1b.

Condition 1. The data subject has given their explicit consent to the processing of the personal data.

Condition 2. The processing is necessary for the purposes of exercising or performing any right or obligation, which is conferred or imposed by law on the data controller in connection with employment.

Condition 3. The processing is necessary: -

- a) in order to protect the vital interests of the data subject or another person, in a case where: -
 - consent can not be given by or on behalf of the data subject, or
 - the data controller can not reasonably be expected to obtain the consent of the data subject, **or**
- b) in order to protect the vital interests of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld.

Condition 4. *For condition 4 to apply you must meet a, b, c and d.*

The processing: -

- a) is carried out in the course of its legitimate activities by any body or association which exists for political, philosophical, religious or trade union purposes and which is not established or conducted for profit,
- b) is carried out with appropriate safeguards for the rights and freedoms of data subjects,
- c) relates only to individuals who are either members of the body or association or who have regular contact with it in connection with its purposes, and
- d) does not involve disclosure of the personal data to a third party without the consent of the data subject.

Condition 5. The information contained in the personal data has been made public as a result of steps deliberately taken by the data subject.

Condition 6. The processing: -

- a) is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings),
- b) is necessary for the purpose of obtaining legal advice, **or**
- c) is otherwise necessary for the purposes of establishing, exercising or defending legal rights.

Condition 7. The processing is necessary: -

- a) for the administration of justice,
- b) for the exercise of any functions conferred on any person by or under an enactment, **or**
- c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department.

Condition 8. The processing is necessary for medical purposes (including the purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services) and is undertaken by: -

- a) a health professional (as defined in the Act), **or**
- b) a person who in the circumstances owes a duty of confidentiality, which is equivalent to that which, would arise if that person were a health professional.

Condition 9. *For condition 9 to apply you must meet a, b and c*

The processing: -

- a) is of sensitive personal data consisting of information as to racial or ethnic origin,
- b) is necessary for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment between persons of different racial or ethnic origins, with a view to enabling such equality to be promoted or maintained, and
- c) is carried out with appropriate safeguards for the rights and freedoms of data subjects.

Condition 10. The personal data are processed in circumstances specified in an order made by the Secretary of State.

7. Schedule 4 Conditions

7.1 Schedule 4 of the Act consists of cases where the Eighth Principle (prohibiting the transfer of personal data outside the European Economic Area) does not apply.

7.2 Schedule 4 provides for circumstances in which the eighth principle does not apply to a transfer. These are where: -

Condition 1. The data subject has given his consent to the transfer.

Condition 2. The transfer is necessary: -

- a) for the performance of a contract between the data subject and the data controller, or
- b) for the taking of steps at the request of the data subject with a view to his entering into a contract with the data controller.

Condition 3. The transfer is necessary: -

- a) for the conclusion of a contract between the data controller and a person other than the data subject which:-
 - is entered into at the request of the data subject, or
 - is in the interests of the data subject, or
- b) for the performance of such a contract

Condition 4. The transfer is necessary for the reasons of substantial public interest. The Secretary of State may by order specify the circumstances in which a transfer is to be taken to be necessary for reasons of substantial public interest.

Condition 5. The transfer: -

- a) is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings),
- b) is necessary for the purpose of obtaining legal advice, or
- c) is otherwise necessary for the purposes of establishing, exercising or defending legal rights.

Condition 6. The transfer is necessary in order to protect the vital interests of the data subject.

Condition 7. The transfer is of part of the personal data on a public register and any conditions subject to which the register is open to inspection are compiled with by any person to whom the data are or may be disclosed after the transfer.

Condition 8. The transfer is made on terms, which are of a kind approved by the Commissioner as ensuring adequate safeguards for the rights and freedoms of data subjects.

Condition 9. The transfer has been authorised by the Commissioner as being made in such a manner as to ensure adequate safeguards for the rights and freedoms of data subjects.

8. Advice and Assistance

8.1 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
1st Floor, Lancaster Circus
1 Lancaster Circus
Birmingham
B4 7AB

8.2 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.

8.3 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