

Director of Legal Services :
David Tatlow

BRIEFING

Local Government and The Data Protection Act 1998

INTRODUCTION

The Data Protection Act 1998 came into force on 1 March 2000. Its purpose is to give individuals rights of access to data held about them and a level of control over how it is used.

In addition it established a new regime for the processing of personal data in virtually all its forms, including most paper records.

Most breaches of the Act constitute offences, and create a right to compensation.

DEFINITIONS

The Information Commissioner

This is the new name for the Data Protection Registrar. She is the person who ensures compliance with the Act and generally promotes good practice amongst Data Controllers.

Data Controller

A Data Controller is any person who determines how data is used and for what purpose. In most cases the Data Controller will be the Council as a whole, but this is not always the case: for example, both School Governors and Head Teachers are subject to obligations to maintain records and will therefore be Data Controllers.

Data Subject

A Data Subject is anybody about whom data is held.

Data

Data means much more than information held on computer. The definition includes "relevant filing systems", meaning, in effect, any paper file containing personal information.

It also includes "accessible public records", meaning education records as defined in Scheduled 11 and housing and social services' records as defined in Schedule 12.

Furthermore, the definition is not limited to facts. It also includes the opinions and intentions of the Data Controller and any other person in respect of the individual.

Personal Data

This means any Data which relates to a living individual who can be identified.

Generally it should be assumed that virtually all information held about living individuals will be subject to the Act.

Sensitive Personal Data

Some Data, by its nature, is considered to warrant extra protection when being

processed. Sensitive personal data consists of information as to:-

- (a) the racial or ethnic origin of the data subject
- (b) his political opinions
- (c) his religious beliefs or other beliefs of a similar nature
- (d) whether he is a member of a trade union
- (e) his physical or mental health or condition
- (f) his sexual life
- (g) the commission or alleged commission by him of any offence, or
- (h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any clause in such proceedings.

Processing

In practice the processing of data means anything that can be done with it, including merely storing it.

THE DATA PROTECTION PRINCIPLES

The Act lists eight principles with which all processing must comply (subject to certain exemptions set out below). The principles are:-

- (1) *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.

Schedule 2 sets out preconditions to the fair and lawful processing of any personal data. They focus on the method by which it was obtained. The condition most commonly relied up will be the Data Subject's consent, but there are others; including contractual obligations, legal obligations and the "legitimate interests " of the Data Controller. This last condition is subject to the requirement that the processing must not interfere with Data Subjects rights under the Human Rights Act 1998.

If the data to be processed constitutes Sensitive Personal Data, one or more of the conditions in Schedule 3 must also be satisfied. These conditions include the explicit consent of the Data Subject, meaning that the consent must be informed, specific and clearly expressed whether in writing or orally. Other conditions require that the processing must be necessary to enable the Data Controller to comply with some statutory requirement, or to protect the "vital interests" of the Data Subject when they are unable to give consent, or it is to be undertaken by a health professional.

The Commissioner has stated that the first principle prohibits a Council from using Council Tax data for any purposes other than the administration and collection of the Tax.

- (2) *Personal data shall be obtained only for one or more specified lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.*
- (3) *Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.*

This should merely be a matter of efficient records management. There is, after all,

no point in asking for data which is either irrelevant or unnecessary for the intended purpose. Nevertheless local authorities have, in the past, been prosecuted for breaching this principle.

- (4) *Personal data shall be accurate and, where necessary, kept up to date.*

Again this is really a matter of efficient record keeping. It will rarely be necessary to keep out of date information.

- (5) *Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or purposes.*

The Commissioner has indicated that she intends to rely on this principle to ensure that Data Controllers give some consideration as to how long they need to retain information. She does not consider it appropriate to provide any guidance of her own on the issue.

- (6) *Personal data shall be processed in accordance with the rights of the data subject under this Act.*

Contravention of the sixth principle only occurs in the following circumstances:-

- Failure to comply with a subject access request.
- Failure to comply with a notice from a data subject exercising the right to prevent processing likely to cause "substantial damage or substantial distress".
- Failure to comply with a notice to cease automatic decision making.

- (7) *Appropriate technical and organisational methods shall be taken against an authorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to personal data.*

This requires Data Controllers to take reasonable steps to ensure the integrity of those staff members who have access to Personal Data. When considering the appropriate levels of security regard should be had to the current state of technological development, the cost of implementation, the potential harm caused by the unauthorised processing or loss of damage to data and the nature of the data itself.

The seventh principle is particularly important when entering into contracts involving the transfer of Personal Data. Any such contract must be in writing and state that any processing must be carried out in accordance with the Data Controller's instructions.

- (8) *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.*

EXEMPTIONS TO THE PRINCIPLES

Most of the exemptions apply to either the subject information provisions or the non-disclosure provisions. The subject information provisions mean the first principle and the rights of access under Section 7.

The non-disclosure provisions mean:-

- The first to fifth data protection principles
- The right to prevent processing likely to cause damage or distress and
- The right to rectification etc in relation to inaccurate data.

The exemptions likely to be relevant to Local Government are set out below.

Crime and Taxation

Data held for the purpose of the prevention or detection of crime, the apprehension or prosecution of offenders or the assessment or collection of any tax or duty is exempt from the first principle and the subject access provisions. The exemption only applies to the extent that compliance with the normal requirements would be likely to prejudice any of the stated purposes. The Benefit Service, Internal Audit and enforcement officers frequently rely on this exemption.

Health, Education and Social Work

The Secretary of State has the power to exempt various classes of data from the subject access provisions. These classes include information relating to the physical or mental health or condition of the data subject, personal data processed by schools and which consists of information relating to pupils at the school and personal data processed by government departments, local authorities or voluntary organisations for the purpose of carrying social work.

Regulatory Activity

Data Controllers are exempt from the subject access provisions where compliance would be "likely to prejudice" various functions designed to protect members of the public in the areas of health and safety at work and financial services.

Research, History and Statistics

A Data Controller is exempt from the subject access provisions and the second principle if the data is used for research purposes. Research can cover anything from market research to scientific research. However, the exemption is subject to safeguards to ensure that the processing is not carried out to support

measures or decisions in respect of particular individuals and that the processing does not or is not likely to, cause substantial damage or distress.

Information Available to the Public

Where the data consists of information which the Data Controller is required to make available to the public whether by publication or making it available for inspection or otherwise and whether or not a fee is charged he is exempt from the subject information provisions, the fourth principle and the right to rectification.

Disclosures Required by Law or in Connection with Legal Proceedings

There is an exemption from the non-disclosure provisions for personal data that are required to be disclosed either by law or by a Court Order.

Some of the more common law requiring the production of personal data are the powers available to benefit fraud investigators and trading standards officers. Another is the "need to know" principle under which Councillors are entitled to certain information.

However, this does not exempt Data Controllers from having to justify their processing under one of the grounds in Schedule 2 and, if the data is sensitive personal data, also under Schedule 3.

Management Forecasts and Negotiations

Management forecasts and negotiations with the data subjects are exempt from the subject access provisions to the extent that compliance would be likely to prejudice the activity or negotiations.

This may include reports prepared with a view to taking disciplinary proceedings against a member of staff.

Examination Marks and Examination Scripts

In the case of examination marks and scripts the period for responding to a subject access request is extended from the usual 40 days to the end of five months after the request is received, or 40 days after the day the results are announced whichever is the earlier.

NOTIFICATION

Any person processing personal data by automated means has to notify the Commissioner of the type of processing he intends to carry out and for what purpose.

In effect the notification constitutes a public declaration by the Data Controller as to his intentions regarding personal data.

RIGHTS OF DATA SUBJECTS AND OTHERS

Rights of Access to Personal Data

Any individual can ask a Data Controller whether they are a data subject in respect of that controller's processing. The Data Controller should then give the Data Subject a description of the data held (which should correspond with the notification entry). In addition the Data Controller must describe the actual purposes to which the data are put, including who will receive the data. This may include other Council departments.

If the data held were used for solely automated decision making the Data Controller must explain the logic involved in the decision taking.

A Data Controller is not obliged to comply with a subject access request unless the request is made in writing and the required fee paid. The Data Controller then has 40 days from when he has sufficient information to comply with the request to do so.

If the Data Controller cannot comply with a request without disclosing information relating to other individuals the consent of those individuals must be obtained, unless it is unreasonable in all the circumstances to do so. This will require a balancing between the impact of disclosure and the effects of a failure to disclose.

Right to Prevent Processing likely to Cause Damage or Distress

The Data Subject has the right to request a Data Controller to refrain from processing any data on the grounds that it is causing or is likely to cause substantial damage or distress to him or another.

However, the Controller is exempt from this in any case where the conditions necessary for fair and lawful processing are met.

Right to prevent Processing for Purposes of Direct Marketing

Any individual is entitled to request, in writing, that the Data Controller refrain from any direct marketing. This would include retaining the records of computerised ticket sales, and the inclusion of advertising material on payslips or mailings included in tenant correspondence.

Rights in relation to automated Decision Taking

An individual is entitled to require a Controller to refrain from any automated processing which significantly affects him. This includes the provision of any Council services on a purely computerised scoring system. However there is an exemption if the decision making is authorised or required under any enactment such as, for example, benefit claims.

Right to Compensation for Failure to Comply with Certain Requirements

If an individual suffers damage as a result of any failure of the Controller to comply

with the Act they may be entitled to compensation. In addition to compensation for damage a further sum can be awarded for distress. However there is a defence on the basis that the Controller did everything reasonably required to comply with the requirement concerned.

Right to Rectification, Blocking Erasure and Destruction

An individual may apply to a Court for the rectification, erasure etc of their details on the basis of the data being inaccurate. It is not necessary to prove that the inaccuracy has led to any damage.

OFFENCES

The Act creates a number of offences. The failure to give notification when required to do so is an offence of strict liability.

It is also an offence to knowingly or recklessly disclose personal data other than in accordance with the Act. A further offence is committed if a person sells any data obtained in this way.

In most cases the individual officer who discloses the data, as well as the Data Controller, will commit the offence.

TRANSITIONAL PROVISIONS

There are two transitional periods before the Act comes fully into force. The wording of the relevant provisions is, unfortunately, extremely complex.

The first period lasts until 24 October 2001, during this time any processing of manual data, and automated payroll data that was being carried out as at 24 October 1998 may continue under the terms of the Data Protection Act 1984.

The second period lasts until 24 October 2007. Until this date manual data forming part of a relevant filing system which was in existence as at 24 October 1998 are

exempt from the first principle (save for the requirement to give notification to Data Subjects) and the second to fifth principles inclusive. As will be apparent this is therefore is a fairly narrow exemption. Few records will be included.

For advice on Local Government and The Data Protection Act 1998 contact Varun Shingari on:-

Tel: 0121 464 3459

Fax: 0121 303 4936

E-mail: varun.shingari@birmingham.gov.uk