NALC

Legal Topic Note

LTN 38

September 2011

DATA PROTECTION

Introduction

1. The Data Protection Act 1998 came into force on 1 March 2000. The Act gives effect in UK Law to the 1995 EC Data Protection Directive. It strengthens and extends the data protection regime created by the Data Protection Act 1984 which it replaces. It provides the statutory framework for the use of computerised information (including microfiche, audio and visual systems) and also certain manual records about living identifiable individuals in the United Kingdom. The Act does not prohibit disclosures of such information to third parties but it regulates the circumstances in which they can be made. It gives enhanced "subject access rights" (see below) and creates a new category of "sensitive information". It also prohibits the transfer of personal data to countries which do not have an "adequate level of protection".

Definitions

2. The 1998 Act again creates its own definitions. The important definitions are: -

"Personal Data" means data which relates to a living individual who can be identified:

- from the data; or
- from the data and other information which is in the possession of the data controller (see below), and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual;

"Data Subject" means an individual who is the subject of personal data;

"Data Controller" means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data is, or are to be, processed;

A data controller must be a "person" i.e. a legal person. This term comprises not only individuals but also organisations such as corporate and unincorporated bodies of persons and indeed companies. In the circumstances it is entirely appropriate for a council in its corporate entity to be the data controller for the purposes of the Data Protection Act.

"Processing" – Processing is very widely defined and it covers almost anything: "retaining, recording or holding……. including organisation, adaptation, or alteration, retrieval, consultation or use, disclosure by transmission, dissemination or otherwise making available, alignment, combination, blocking, erasure or destruction of the data."

Data Processing – The Eight Principles

3. The Data Protection Act applies to 'personal data' which is, as stated above, data about identifiable living individuals. Those who decide how and why personal data is processed (data controllers) must comply with the rules of good information handling, known as the data protection principles, and the other requirements of the Data Protection Act. There is not, in fact, a lot of difference between the principles, which were set out in the 1984 Act, and those now contained in the 1998 Act. There are still eight in number but the text of the first seven contains slightly more detail that the original set.

4. The eighth principle in the 1998 Act did not appear in the 1984 Act and relates to the prohibition on transferring personal data to countries that do not have an adequate level of protection.

i. The rules of good information handling – the principles

5. Anyone processing personal data must comply with the eight enforceable principles of good practice. They say that data must be:

- processed fairly and lawfully and such processing must comply with at least one of a set of specified conditions (see below). Additional conditions apply to sensitive personal data;
- obtained only for one or more specified and lawful purpose, and shall not be processed in any manner incompatible with the purpose or those purposes;
- adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed;

- accurate and where necessary, kept up-to-date;
- not kept for longer than is necessary for the purpose or purposes for which it was processed;
- processed in line with the rights of data subjects under the Act;
- 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; and
- not transferred to a country or territory outside the European Economic Area (EEA) 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.

ii. Processing personal data

6. As stated above "processing" is broadly defined and it takes place when any operation or set of operations is carried out on personal data. The Act requires that personal data be processed "fairly and lawfully". Personal data will not be considered to be processed fairly unless certain conditions are met. A data subject is also entitled to know the identity of the data controller and why information is, or is to be, processed.

7. Processing may only be carried out where one of the following conditions has been met:

   - the individual has given his or her consent to the processing;
   - the processing is necessary for the performance of a contract with the individual;
   - the processing is required under a legal obligation;
   - the processing is necessary to protect the vital interests of the individual;
   - the processing is necessary to carry out public functions; or
   - the processing is necessary in order to pursue the legitimate interests of the data controller or third parties (unless it could prejudice the interests of the individual)

8. In our opinion local councils will be able to rely on several of these conditions in ensuring they comply with the Act.

iii. Processing sensitive data

9. A data controller who processes sensitive personal data must comply with one of the conditions listed in the Third Schedule to the Act. It is thus vital for data controllers to check all sensitive processing (if any) to see that it complies with one of the provisions

listed. Sensitive personal data is personal data consisting of information as to – racial or ethnic origin; political opinions; religious or other beliefs; trade union membership; physical or mental health or condition; sex life; criminal proceedings or convictions.

10. Sensitive data can only be processed under strict conditions which include;

- having the explicit consent of the individual;
- being required by law to process the data for employment purposes;
- needing to process the information in order to protect the vital interests of the data subject or another;
- dealing with the administration of justice or legal proceedings.

Paper files/manual records

11. The most significant change from the 'old' law is that manually processed information is included in the definition of 'data'. Whereas the 1984 Act regulated the handling of electronic data only, the 1998 Act relates not only to automatically processed information but also to information which forms part of a "relevant filing system".

12. The Act describes this as any set of information structured by reference to individuals or that can be accessed by reference to criteria relating to individuals. This definition means a significant amount of manual data falls within the scope of the Data Protection Act as does the extension of the definition of data to cover 'accessible records'. Accessible records are broadly school pupil, housing, social services and health records to which access was previously available under other legislation.

13. The Information Commissioner (see below for address) has described a "set of information" as comprising a group of things under a common heading or identifier. Files headed: Contacts and Complainants for example could meet the criteria.

14. The personal data must also be capable of being accessed by reference to the individual or criteria relating to the individual. For example, the individual's name, a correspondence ref. number, or a file number, address, age, or membership of an organisation.

15. Files concerned with matters of council policy are unlikely to fall within this definition.

Rights of Data Subjects

16. A person about whom information is held (a 'data subject') is entitled (usually for the payment of a fee of £10) to be informed by any 'data controller' whether any information is held on him / her and to:

    - a description of the data; and
    - a copy of the information in an intelligible form.

17. The data subject is also entitled to request and receive information pertaining to:

    - the purposes for which the data is being held;
    - the recipients or classes of recipients to whom is may be disclosed; and
    - the source of the data.

18. If the data has been processed by a computer in order to arrive at a decision and the outcome of such processing significantly affects the data subject, the individual concerned is entitled to be informed of the logic behind the decision – making process.

19. Where the processing of a data subjects personal data causes unwarranted and substantial damage or distress s/he is entitled to send a notice (the 'data subject' notice) to the data controller requiring the latter to cease such processing.

20. The data controller must, within 21 days, send the data subject a written notice stating that the request has been complied with or the reasons why he feels the data subject notice to be unjustified. Inadequate compliance with a data subject notice may be remedied by court order.

21. Similar provisions exist in respect of direct marketing personal data, in that a data subject can request a data controller to cease processing such data. Direct marketing is advertising or marketing material directed at individuals and therefore includes 'junk mail'.

22. Individuals also have the right to have wrong information corrected, blocked from processing or erased.

Notification

23. Registration under the 1984 Act is replaced with notification. Most organisations (including local councils) will need to notify the Information Commissioner in broad terms, of the purposes of their processing, a description of the personal data processed, the recipients of the personal data processed and the places overseas to which any data is transferred. This information is made publicly available in a register. The processing of personal data without a notification is an offence punishable by a potentially unlimited fine. Notifications are renewable annually.

Exemptions

24. The 1998 Act does not apply to data processed for the purposes of safeguarding national security or for purely personal, family or household purposes.

25. Similar exemptions exist for data held for the prevention or detection of crime and for the assessment or collection of taxes as well as certain 'regulatory activities'. Section 31 of the Act gives exemption to certain journalistic, literary or artistic material. This is not an exhaustive list.

As far as local councils are concerned exemptions may be available for certain specific circumstances namely:

- Where personal data is processed for one or more of the following purposes **only:**
  - staff administration (including payroll),
  - advertising, marketing and public relations (of the council itself); or
  - accounts and records;
- Disclosures required by law;
- Where disclosure is necessary for the purpose of legal proceedings or for obtaining legal advice;
- Legal professional privilege (i.e. confidentiality between client and professional legal adviser); and
- Where the sole purpose of any processing is the maintenance of a public register (e.g. the register of members interests under the Code of Conduct).
- Where no personal data is processed by computer.

26. Even where there is no requirement to notify the following will still impact for data controllers:

    - The rules of good information handling ("the eight principles") surrounding the processing of personal information must still be observed;
    - The rights of data subjects (the person who is the subject of the information) must still be complied with and,
    - The Information Commissioner can still step in should they believe there has been non compliance/ a breach by a council.

Penalties

27. If the Information Commissioner is satisfied that a data controller has breached the legislation it is open to that Office to serve an enforcement notice requiring compliance. Failure to comply with such a notice can be a criminal offence punishable with a fine.

28. In addition, the court and Commissioner have power to award compensation to data subjects who suffer damage and distress as a result of any contravention by a data controller of any of the requirements of the Act.

How does the Act affect local councils?

29. Whilst exemptions to the requirement to notify exist (as outlined above) NALC takes the view that local councils will be hard pressed to argue that all their data processing falls within the scope of those exemptions. In short this is because local councils (like all local authorities) hold such a wide range of information.

30. Accordingly, councils will ordinarily need to take steps to "notify" (if they have not already done so). To reiterate this will mean councils forwarding to the Information Commissioner:

    - The council's name as the data controller (with a named contact within the council and that person's contact details);
    - The reasons why it is holding or processing data;
    - Whether the data will be disclosed, and to whom,
    - The names of any countries outside the EEA to which data may be transferred;
    - Details of how data will be kept secure.

31. The annual fee for notification is £35. Councils wishing to notify can either do so by contacting the Information Commissioner (see below for contact details) or on line at www.ico.gov.uk

32. It is clear that councils are affected by the provisions of the Data Protection Act in a multitude of ways. "Personal data" may be as simple as holding someone's name and address but in addition includes amongst other things details of complaints, lists of contacts, employee/personnel records and information provided for the purpose of placing a contract to which the data subject is a party. Images taken by CCTV systems can now also fall within the data protection regime.

33. The following are a number of practical considerations which a council may wish to bear in mind to help ensure it complies with the Act: -

    i. It should firstly look at any data it holds to see if it includes personal data. Particular attention should be given to such things as contractor/supplier lists where there are businesses involved as they could contain personal data as many businesses are owned by sole traders or partnerships. Even with companies, a council may store personal data on contacts at the company. Councils which hold personal data will of course need to notify the Information Commissioner.
    ii. It should be noted the Act only applies to the "processing" of personal data but processing is so widely defined it will in fact catch almost any conceivable operation on such data.
    iii. A council should (if appropriate) consider where it obtained any personal data from: unless it can prove it was obtained fairly there is a risk the law will be broken. What constitutes "fairly" is somewhat complex but it includes the data subject consenting to the council using it i.e. was the data subject originally told their data might be given to third parties?
    iv. A council should ensure that individuals are aware of the uses that will be made of the information they supply and give their consent to that specific use. Where the use is obvious (e.g. name and address for correspondence purposes) or is a legal requirement the consent need not be explicitly obtained. Where there is no clear purpose then consent should be obtained.
    v. Data should never be given (or sold) to anyone else unless the data subject has given his/her consent or there is, by law, a duty to do so. Use of personal data on a website will automatically be a breach of the Act unless express consent has been given.

vi. A council obtaining consent to any use – whether express or not – should make sure that it is "informed consent" i.e. that is been made very clear exactly what the council intends using the data for and what data it is holding.

vii. A council should ensure it only keeps the bare minimum amount of information necessary for its purposes. It should carry out regular reviews to check that all of the information asked for on such things as application forms or registration forms really is required and necessary.

viii. All data recorded must be accurate and where necessary kept up-to-date and deleted when no longer required.

ix. The information must be kept safe and secure at all times. The level of security will depend upon the sensitivity of the data involved. Listed below are some good practice points:

Manual records

34. Filing cabinets must be locked outside of normal working hours and keys must be held securely by nominated staff. All papers should be securely locked away when not in use to prevent other people from inadvertently gaining access.

Computerised records

35. The following guidelines apply:

- Access should be controlled by unique password and passwords should be changed on a regular basis;
- Passwords and access controls should be kept secure when not in use;
- Personal information should not be left displayed on screen when not in use;
- Floppy discs/CD ROMS should be filed away securely and not left lying around;
- If the personal information is held on a lap-top computer this should be locked away when not in use;

Elected members:

36. Where holding and processing personal data about individuals in the course of undertaking council business elected members will be covered by the authority's notification and have the same responsibilities with regard to data protection as an employee of the authority. Elected members who process electronic personal data in an individual capacity (i.e. where they are not acting on behalf of their council) are likely to qualify as data controllers and they would individually need to notify the Information

Commissioner's Office. Please see the NALC legal briefing issued in 2011 for further information on councillor notification.

Further Information

37. Responsibility for managing the notification scheme, enforcing the Acts requirements and promoting compliance and good practice lies with the Information Commissioner who's address is: -

Office of the Information Commissioner
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Information Line:	01625 54 57 45/ 08456 30 60 60
Switchboard:	01625 54 57 45
Fax:	01625 52 45 10
Website:	http://www.ico.gov.uk/

The Information Commissioner provides advice and publishes useful guidance on the Act and can be consulted if a council is in doubt as to whether or not it needs to "notify".

Other Legal Topic Notes (LTNs) relevant to this subject:

LTN	Title	Relevance
37	Freedom of Information	Sets out the information councils are obliged to disclose.
40	Local Council Documents and Records	Sets out the documentation councils should retain for legal and other purposes.