

# DATA PROTECTION

## PART 2: NOTIFICATION AND SECURITY OF PERSONAL INFORMATION

**Jacqueline Gazey is an experienced and ISEB accredited data protection practitioner who has over six years experience in the practical application of privacy law. She has developed procedures, policy and tools to meet the requirements of both the 1984 and 1998 Data Protection Acts.**

**Jacqueline is the co-author of the BSI guide to Subject Access and has been involved in the regularly held ISEB accreditation training courses, run by the BSI. She frequently writes about the practical application of data protection law for trade publications and specialist periodicals and, as a data protection consultant, has a wide range of experience in delivering practical training, guidance material and compliant working procedures.**

**This article is intended as a high level overview of the 2nd and 7th Data Protection Principles. Full information about the Act and its interpretation can be obtained from the Information Commissioner.**

**Key words: data protection, eight principles, patient records, privacy, individual's rights**

**U**nder the Data Protection Act 1998, the 2nd principle states: "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".

From this principle comes the requirement that organisations must register or 'notify' the processing\* of any personal data, with the Information Commissioner's office (the governments appointed Regulator of data protection).

This article covers what type of information needs to be notified and the process for notifying. As such it may seem strange to then link this to the 7th Data Protection Principle which states that appropriate technical and organisation measures should be taken to protect personal data from unauthorised or unlawful processing or accidental loss or destruction.

The reason for the link is that when notifying processing to the commissioner's office, organisations are

asked to make a simple declaration as to the security measures that are in place to protect personal information. These are yes/no answers but to answer in the negative will indicate that the organisation is breaching the Data Protection Act.

The requirement to register has been in existence since the 1984 Data Protection Act came into force. Under the original Act, there was a small technical flaw in the law that meant that if organisations failed to register with the [then] Data Protection Registrar, the only aspect of the law they could be prosecuted for was failing to register. Any other breach of the Act had to be let go. This has been rectified under the new legislation and the process simplified.

### What is notification?

The Information Commissioner is required to maintain a public register of 'data controllers'. Each registered entry shows the name and address of the organisation concerned, together with a general description of the data they process, what it is used for and to whom it may be disclosed. All organisations that process personal information must notify – unless they are eligible for an exemption. Optical practices would not be eligible for such an exemption because of the medical/health data they process.

As mentioned, the notification procedure is reported to be a simplified version of the old registration requirement and if an organisation was registered under the 1984 Act, they will be sent a draft conversion from the registration format to a notification format about six weeks prior to their registration's expiration. These old style registrations will run through to around the end of 2003 as organisations could register for three years at a time with the old system. The new notification system only allows for an annual registration.

### What must be notified?

Organisations are required to notify the following information:

- The name of their organisation (data controller) whether they are sole traders, partnerships, limited or public limited companies, schools or voluntary bodies.
- The data controller's address. For limited companies, this should be the registered office address. For other style businesses this can be the principal place of business.
- Company registration number
- Contact details
- A description of the processing of personal data. This is categorised by specific 'purposes' and for each 'purpose', information has to be given on the data subjects, the data classes, the recipients and where transfers are made.
- A security statement. This is a statement that is intended to identify an

organisation's commitment to data security and links directly to the 7th principle.

## How to establish what should be notified

For an organisation to ascertain what categories should be notified to the Information Commission it needs to look at what data it uses, how it uses it, to whom it might disclose information and whether it processes any data outside the EEA. Remember that the Isle of Man and the Channel Islands are not part of the EEA.

Then look at the template notification available from the Information Commissioner. This identifies the main purposes as:

- Accounts and Records (eg, keeping accounts relating to any business or other activity, purchase and sale records, payment and delivery notices, provision of services etc)
- Health administration and Services (defined as the provision and administration of patient care)
- Staff Administration (defined as appointments or removal, pay, discipline, superannuation, work management or other personnel matters in relation to the staff of the data controller).

To this template it may be necessary to add additional purposes – such as:

- Advertising, marketing and public relations (especially if the organisation uses reminder cards to promote any goods or special offers)
- Crime prevention and prosecution of offenders (mandatory if the organisation has CCTV installed)
- Trading / sharing in personal information (defined as the sale, hire, exchange or disclosure of personal data to 3rd parties in return for goods/services /benefit).

The Information Commission has made a guide available which outlines all of the established purposes they consider important. However, there is also a provision to 'make up' purposes if none of the pre-defined ones seem to apply.

Having established which purposes are relevant, each purpose then needs to record Data Subject, Data Classes, Recipients and Transfer information

**Data Subjects:** These are, quite simply, the subjects of the personal data – such as 'Customers and Clients'. Again, the guide gives 10 established descriptions. However, as with all these sub-categories, there is no facility to 'make up' new ones if these don't appear to apply, so the given descriptions must be used.

**Data Classes:** These represent the type of data that are being processed. There are 14 given categories.

**Recipients:** These indicate the type of individuals or organisations that personal information are disclosed to. There are 26 categories.

Transfers of Personal Data. This is to

show which Countries personal data may be transferred to. Whilst the act doesn't specifically define 'transfer' the Commission recommends the ordinary meaning of the word – ie the transmission from one place/person to another. This will therefore include posting information on a website that can be accessed from overseas. The choices are

- None outside the EEA
- World-wide (although some explanation as to why this option has been selected may have to be given)
- Specific countries. The guide suggests that if the specific countries add up to more than 10, the worldwide option should be taken.

Use the Commissioner's template as a starting point, but remember that it only covers the barest minimum and should be expanded to cover each organisations processing.

## How to notify

After ascertaining all the purposes, data subjects, data classes, recipients and worldwide transfers these need to be notified to the commissioner. This can be done:

- Over the Internet. Complete the on-line form, print it off, sign it and post it to the Commissioner's office with the £35 fee.
- By telephone. The Commissioner's office record all the details, post out a copy of the notification for checking, signature and return with fee
- Request a notification application form from the Commissioners office. This is sent in the post and needs to be completed by hand, signed and returned with the fee.

## The Security Statement and the 7th Principle

The 7th Data Protection 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 Notification form requires that data controllers give a general description of the measures they take to meet the obligations of this 7th by asking: "Have you taken any measures to guard against unauthorised or unlawful processing of personal data and against accidental loss, destruction or damage? Yes/No"

If you answer "no" to this question, you are categorically in breach of the data protection act 1998.

The statement then goes on to ask. "If Yes, please answer the following question", "Do the methods include":

1. Adopting an information security policy. This is defined as providing clear management direction on responsibilities and procedures in order to safeguard personal data. In reality it means that organisations should know what steps it

takes to protect information and ensure that all members of staff are aware of these.

2. Taking steps to control physical entry. Eg: Intruder alarms, restricted access to areas where records are held etc.
3. Putting in place controls on access to information. Eg: Password protection to electronic data, encryption etc.
4. Establishing a business continuity plan. Eg: holding back up files of electronic data, manual files held in fireproof cabinet's etc.
5. Training your staff on security systems and procedures. This is one of the main ongoing steps organisations can take to protect themselves from prosecution. If staff know their obligations and receive regular reminders, the Data Controller will be seen as acting responsibly and any breach could then be put down to human error – which can always happen and the Information Commission accepts.
6. Adopting the British standard on information security management BS7799. This is the only question that organisation can answer "no" to and still remain compliant with the law.

Overall, the intention of the Commissioner's office is to promote the setting and documenting of business Policy and Procedures for complying with the data protection act and the ongoing training of staff in these procedures. In reality, most small businesses are not going to have the time or expertise available to develop these. The most important aspects therefore are that standard measures are in place (although not necessarily documented) and that members of staff are aware of the basic requirements of the Act.

To support the awareness aspect, the Commissioner's office produces training videos and guidance booklets, which explain the Act in its basic form. These are available- in most cases free of charge – from the Commissioner's office.

## References

1. Schedule 1, part 1, principle 2 of the 1998 Data Protection Act.
2. EEA = European Economic Area: Austria, Belgium, Denmark, France, Finland, Germany, Greece, Iceland, Ireland, Italy, Liechtenstein, Luxembourg, The Netherlands, Norway, Portugal, Spain, Sweden, UK.
3. The Notification Handbook - available from the Information Commissions Office, Wycliffe House, Water Lane, Wilmslow SK9 5AF; telephone 01625 545745.
4. Schedule 1, Part 1, Principle 7 of the 1998 Data Protection Act.
5. Items 1-6 are lifted verbatim from the 1998 Data Protection Act Notification Application Form.
6. Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow SK9 5AF; telephone 01625 545745. ■