

# DATA PROTECTION

## PART 3: INDIVIDUAL RIGHTS

**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.**

**Under the 1998 Data Protection Act, Principle 6 states that 'Personal data shall be processed in accordance with the rights of data subjects under this Act'**

**U**nder the 1998 Data Protection Act, Principle 6 states that '*Personal data*\* shall be processed in accordance with the rights of data subjects under this Act'. This is because the Act gives individuals certain rights over their personal information. These rights are:

1. Rights of access to *personal data*
2. Rights to prevent *processing* likely to cause damage or distress
3. Rights to prevent *processing* for the purpose of direct marketing
4. Rights in relation to automated

decision-taking

5. Rights to have inaccurate *data* rectified, blocked, erased or destroyed
6. Rights to compensation for failure to comply with the requirements of the Act.

With the majority of these rights, there are specific response times laid down within the law that organisations must comply with. As such, it's important that business ensures that employees are able to recognise requests to give their organisations the maximum time available to respond.

### Rights of access to personal data

This right is arguably one of the most important and most well publicised rights under this Act. The previous data protection law allowed for access to information but this only covered electronically held data. This Act now includes a right to manual records as well as other information – such as where data has been collected from, what it's processed for and to whom it may have been disclosed.

Where an individual asks an organisation for a copy of any personal information they may hold on them, the organisation has **40 calendar days** to provide that information. These requests have to be made in writing, however, and before meeting such requests; an organisation has the right to:

- Request any information from the applicant that may reasonably be required to locate the personal data. An application form might be the preferred approach as this could be used to establish what exact information the applicant is looking for and thereby limit the request to specific data rather than 'everything held'.

- Charge a fee of up to £10

- Request information to satisfy themselves as to the true identity of the applicant

Until these three aspects have been met, the 40-day time limit doesn't have to start.

For organisations to comply with this right under the Act, they will need to have an established process in place to handle requests within the statutory time limit. To develop this process, the organisation should consider:

- Nominating a single member of staff as the primary point of contact
- Identifying all the areas where personal information are processed (patient record cards, electronic reminder systems, CCTV, copies of NHS documentation, staff records, CVs from potential members of staff etc).
- Establishing how long it may take to retrieve any information and convert it into an understandable, permanent format

- Whether to use an application form, charge a fee and what identification/verification information is acceptable

Once these areas have been considered, a process can be established to handle any such requests.

### Recognising requests

Firstly, for requests to be valid, they have to be made in writing. This includes electronic requests – such as e-mail or fax. It should be a request to access personal information relating to the applicant. It may mention the Data Protection Act or the Information Commissioner (but does not have to).

The application must be made by the individual concerned or by a person authorised to act upon their behalf and finally can be limited to specific information or encompass all information held.

## Procedures

Here are some activities that should be undertaken prior to instigating a request for access. These activities should be carried out promptly as they cannot be used as a delaying tactic to hold the 40-day clock back.

- Ascertain what information the applicant requires.
- If medical information is required you may need authority to disclose the information from a health professional
- If the data identifies another individual you may need their authority to disclose their information to the applicant.
- Ask for proof of identity. This may take the form of documented evidence or a face-to-face verification if the individual is known to the organisation
- Take a fee – if it's been decided to charge one. Consider taking a fee – you can always refund it in the spirit of good customer service if you choose.

After fulfilling the above elements, start collating the information required and confirm to the applicant when they should expect to receive the data.

Once the information has been collected together, check it for inaccuracies, reference to other individuals or health data.

If inaccuracies are found, the preferred approach is to provide the incorrect version with an explanation that the inaccuracy has been spotted. For public authorities this is the only course of action available as amending the records prior to their release to the applicant is an offence under the Freedom of Information Act 2000<sup>1</sup>.

Reference to other individuals may require that person's consent. Alternatively, it may be possible to edit or mask this information to protect the other party's identity. Failing these two actions, consideration needs to be given as to whether (a) there is a duty of confidentiality to the 3rd party or (b) whether the applicant's right to see this information outweighs the other party's right to privacy.

Health data is subject to provisions of secondary legislation<sup>2</sup> which states that organisations should consult an appropriate health professional before providing previously unreleased medical or health data – where that data may cause serious harm to the physical or mental health (or condition) of the applicant, or indeed any other individual. This may be a very onerous obligation for organisations to undertake. If the health professional is outside the optical practice concerned, it may be difficult to ascertain who the appropriate health

professional is. They may charge a fee and have no duty to respond within the required time limit.

## What data could be retained?

There are a number of exemptions that can be applied to enable information to be withheld. However, before any data is refused, careful consideration should be given to the retention and the reasons why data have not been disclosed should be documented, in case the organisation is asked to justify withholding information to the Regulator.

The following information could be withheld and not disclosed under requests for subject access:

- Confidential references - given in confidence
- Information that is intended to be used in negotiation with the applicant
- Self-incriminating information
- Information that would prejudice crime prevention, detection, apprehension or prosecution of offenders or the assessment or collection of tax or duty
- Information subject to legal professional privilege
- Examination scripts & examination marks (the academic or professional records of candidates made under exam conditions)

Once the information is ready for release, it's recommended that it be issued by recorded delivery to document the date of issue and ensure delivery.

## Rights to prevent *processing* likely to cause damage or distress

Where an individual believes that *processing* of his personal information will cause substantial damage and distress to himself – or another individual – he can write to the organisation concerned with a demand to cease that *processing*. This demand must specify the reason the individual believes why the *processing* is (or is likely to) cause damage or distress.

Where an organisation receives such a demand, it must **respond within 21 calendar days** stating either it has or intends to comply with the notice or outlining the reasons why it believes the demand to be unjustified.

## Rights to prevent *processing* for the purpose of direct marketing

This right states that an individual is entitled at any time – by notice in writing to an organisation – to require that organisation to stop (or never start) using his personal information for direct marketing purposes.

The Act defines direct marketing as a communication, by whatever means, of any advertising or marketing material which is directed to a particular individual. However, the Information Commissioner (the government's appointed Regulator) has a different view. The Commissioner's view is that direct

marketing is any activity that promotes the goods, services or image of an organisation. This would include such activities as charity donation requests or even encouraging the public to lobby their local MP over a given subject<sup>3</sup>. This is obviously a much wider interpretation than the definition in the Act. This means that such activities as sight test reminders could be viewed as marketing activity, if not initially positioned with the patient correctly – say, as an integral part of the service. Should an organisation take these notices as an opportunity to highlight any special promotions – such as free sight-tests or a buy one get a spare pair free offer – these communications are immediately taken out of the service style notice into a marketing communication.

In order to combat any misinterpretation, sight test reminders should be positioned as an agreed service provided by an optician and an important aspect on continued good eye health. If, however, it is intended to use reminders as a marketing tool, then the organisations concerned should expect to get some patients 'opting-out' and be prepared to record these in a manner that can be cross-referenced against future marketing activities to ensure their names are removed.

## Rights in respect of automated decision taking

An individual is entitled to ask an organisation – again this has to be in writing – not to make any 'significant' decisions solely by automated means. Whilst 'significant' is not really explained, the intention is for activities such as measuring an individual's work performance, creditworthiness, reliability or conduct.

If an organisation receives such a request from an individual, they have **21 calendar days to respond** with what steps they intend to take to comply with the notice.

## Rights to have inaccurate data rectified, blocked, erased or destroyed

This section of the Act mainly revolves around what is required by organisations if the courts find them to be in breach of data protection legislation in processing inaccurate data. The reality is that no organisation wants to get into a position where such an issue gets to the courts. It is therefore practical to have a method to correct inaccurate information – whether this is held in electronic or a manual format.

This right also highlights why it is important to record any instances where personal data are passed on to other parties. It falls to the organisation that originally held the incorrect data to ensure that the records of any other parties they have disclosed the information to are amended.

### Rights to compensation for failure to comply with the requirements of the act.

Any individual who suffers damage or damage and distress (damage is defined as financial loss or physical injury) as a result of any breach of the Data Protection Act is entitled to claim compensation from the 'Data Controller'.

An example could be an optician who has made up spectacles for two patients called Mr J Brown and Mr S Brown. When Mr J Brown comes to collect his glasses, he is incorrectly handed those intended to Mr S Brown. He leaves the practice with the new glasses, puts them on as he gets into his car and immediately has an accident as he thought the space between his car and a parked car was much wider. In this scenario, Mr Brown has incurred financial loss, through the damage to two cars, possibly has a physical injury and may even be able to claim distress.

Compensation is not payable for distress alone, unless the data has been used for the 'special purposes' (journalism, literary, or artistic purposes). However, if the organisation concerned can prove that it had taken reasonable care in all the circumstances to comply with the relevant aspect of the Act, this could be sufficient defence.

'Reasonable care' for an optical business could be construed as ensuring staff are aware of their obligations, through training, reminders, clear procedures for handling personal information and keeping it secure.

Lastly, whilst not such a formal right under the Act, individuals also have the right to request the Information Commissioner to make an 'assessment' as to whether processing may be in contravention of the Act. In reality, this 'assessment' acts as a legalised complaint process. When the Information Commissioner receives a request from assessment, there are a couple of different approaches that may be taken. It may be that there has clearly been a breach of the Act and the Commissioner will write to the organisation concerned to inform them of this fact, and advise what action they need to take. Alternatively, the Commissioner may write to the organisation concerned to establish what their procedures and policy is. In these cases, there will be a designated time period in which the organisation must respond. Once this response has been received, the Information Commissioner will then make a judgement as to whether a breach of the Act has occurred and what actions need to be taken by the parties concerned.

The above information is a high-level overview of the rights granted to individuals under the Data Protection Act 1998 together with some

recommendations for handling subject access requests. Full information relating to the obligations of data controllers in this regard can be found in the Act <sup>4</sup> itself and from the Information Commissioner's office <sup>5</sup>.

### References

1. FOI Act 2000 - Section 77.
2. Statutory instrument 2000 // 413. The Data Protection (subject access modification)(Health) Order 2000.
3. Information Commissioner's 'Legal guidance' document on the 1998 Data Protection Act.
4. Data Protection Act 1998 - ISBN 0 10 542998 8
5. [www.dataprotection.gov.uk](http://www.dataprotection.gov.uk)

\* Italic words relate to 'definitions' outlines in *Data protection, Part 1: an overview*, *Dispensing Optics* April 2003. ■