Complying with the Data Protection Act Checklist 220

Introduction

Almost all managers will come across data protection issues at some point in their working life. In the UK, the Data Protection Act 1998 (DPA) is the main source of law on issues regarding data protection and is designed to balance the legitimate need of organisations to collect and use data for business purposes with the right of individuals to gain access to their personal data. It is also about recognising data as a valuable asset and safeguarding that asset.

There are very few commercial organisations which do not need to register under the Data Protection Act. Registration is relatively easy and cheap, although from 1 October 2009, a two-tiered structure of notification fees, based on organisation size and turnover has been introduced as follows:

- a notification fee of £500 now applies to data controllers of organisations with a turnover of £25.9M and more than 249 members of staff and of public authorities with more than 249 members of staff.
- all other data controllers remain in the lower-tier category, paying £35 per annum unless they are exempt.

Registered charities and small occupational pension schemes do not come into the higher-tier, regardless of their size and turnover, and remain in the lower-tier unless exempt from the requirement to notify altogether. The notification fee is currently exempt from VAT. Failure to register and/or keep the registration up to date is a strict liability criminal offence, against which there is no effective defence.

What is the Data Protection Act?

The UK Data Protection Act implements the European Union Data Protection Directive 95/46/EC and every country in the European Economic Area (EEA) has implemented the same directive – the EEA constituting all EU countries plus Norway, Iceland and Liechtenstein. The Channel Islands and the Isle of Man are not inside the EEA.

The DPA regulates the processing of information relating to individuals (and can cover emails, CCTV images, membership information, photos etc). This includes the obtaining, holding, using or disclosing of such information, known as personal data. It covers manual filing systems and records as well as computerised ones, card indexes and microfiche.

Personal data is defined by the Data Protection Act 1998 as data relating to a living individual who can be identified from that information, e.g. name, address, and telephone number.

Sensitive Personal Data includes information on racial or ethnic origin, political opinions, religious beliefs, trade union membership, physical or mental health, sexuality and criminal convictions.

There is an extra layer of safeguards for the use and storage of sensitive personal data - express permission needs to be gained, such as explicit consent from the data subject, or if it is a requirement of employment law.

Action checklist

1. Understand whether the DPA applies to your organisation

Unless you are covered by a legal exemption, the answer is generally yes. Exemptions include some not-for-profit organisations, the maintenance of a public register, the processing of data for personal or family use, and those who only process data for staff administration, advertising, marketing and public relations or accounts and records. Exemptions also apply if you do not process data on a computer. The term computer, however, includes machinery with electronic memories, automatic operation, CCTV and video or sound recording, phone logging and electronic flexi-time systems.

If you are exempt you do not need to notify, but you still need to comply with the other provisions of the Act. Even if you are exempt, it may be of benefit to notify, if only for peace of mind.

2. Understand what the DPA covers

Very broadly it covers information relating to an identifiable living individual, irrespective of whether they are an employee, customer, marketing target or supplier. It does not cover organisations, unless a person from that organisation is named in a database in association with it.

3. Understand the Principles of Data Protection

These are the building blocks of the whole Act. They summarise the Act in 8 principles:

Principle 1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:
i) at least one of the conditions in Schedule 2 is met; and
ii) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

Principle 2. 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.

Principle 3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

Principle 4. Personal data shall be accurate and, where necessary, kept up to date.

Principle 5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

Principle 6. Personal data shall be processed in accordance with the rights of data subjects under this Act.

Principle 7. 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.

Principle 8. Personal data shall not be transferred to a country or territory outside the European Economic Area (EEA) unless that country or territory can guarantee an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

4. Introduce processes and procedure to ensure compliance with the DPA

When introducing processes and procedures to ensure that data is handled in compliance with the DPA throughout the organisation, an implementation plan is a useful tool which will enable you to timetable, build and chart progress, allocate resources and define responsibilities for action. When agreeing the timetable allow for the fact that people will be new to the process and it will take a while to establish useful knowledge.

A good method is to adopt the Plan – Do – Check – Act model.

- Plan actions using the DPA as a guide
- Do what you plan
- Check the progress of actions; do you need to take corrective action?
- Act on your findings

5. Appoint a data controller

Appoint a suitable manager to take on the role of data controller. This will be the person who decides how data is processed and for what purposes. This is not a dictatorial position as the data controller will need to work closely with the data processors to ensure processing meets organisational requirements and complies with the Act.

6. Involve your staff

As staff will carry out most of the data processing, their role is very important. Find out how processing is carried out, look for possible contraventions against the Act, note examples of good practice and decide whether these can be implemented elsewhere. Inform staff that they must not make derogatory or inflammatory comments about other people in emails or on databases as data subjects have the right to see these if they so request and such comments could lead to prosecution.

7. Be clear about the databases you have

It is very important to know how and where personal data is stored within your organisation. The most obvious are computer databases, servers and filing cabinets, but storage also covers information held in personal organisers, card indices, business card folders, emails, voice recordings and security surveillance systems - in fact anything from which a living individual can be identified.

8. Find out for what purposes you process data

The Information Commissioner will require you provide the following information:

- the purposes for which you process data. A standard list is available but if you feel that is not a true description then you can use your own words
- the types of data subjects to which the data belongs, including current, past or prospective data subjects
- the classes of data being processed. Some data is classed as sensitive and if you process these types then you must notify that you do. These include racial or ethnic origin, political opinions, religious beliefs, physical or mental health. Again, a standard list is available from the ICO
- who receives the processed data - whether it is the data subject or another person?
- whether data is sent outside the EEA. American owned companies for instance may send personnel data to their head office or processing is carried out abroad as a result of an outsourcing contract. Personal information can be transferred freely to countries outside the EEA where the European Commission has decided that they have laws similar to those within the EEA.

9. Establish contracts with data processors

Any external data processors you use also need to comply with your requirements. The recommended method for handling this is to establish Data Processor Contracts with them. Most organisations that process data should already have data protection policies and registration in place. However, you will still need to stipulate what you require them to do, and what they may not do. Data security is very important; methods of data transfer must be secure to prevent data, inadvertently or otherwise, falling into the wrong hands. It is important to note, however, that the host organisation remains legally responsible for all personal data under the DPA and that this responsibility cannot be transferred to a third party organisation even if a contract is in place.

10. Prepare a Data Protection Statement

This is the key company document which states the organisation's commitment to following the DPA. There are many examples available, on the internet for example, each one specific to a particular organisation. The statement gives a brief description of how the organisation gains, processes and distributes data whilst ensuring the DPA is followed. Most include option boxes which data subjects can check if they agree or do not agree to certain types of processing, for example, direct marketing. You should also refer to the Privacy and Electronic Communications Regulations 2003 which cover electronic communications and the rights of individuals to opt out of this type of contact. This aspect includes use of mobile communications, including text, sound, images and video – including CCTV systems - as well as facsimile machines and conventional computer based information systems.

11. Notify the Information Commissioner

When you have completed all the steps above, notify the Information Commissioner. A direct debit can be setup to ensure renewal, although the ICO notifications department will let you know in good time when you are due to renew your registration. If anything changes during the year, let the Information Commissioner know so that your details can be changed.

Whilst undertaking notification you will also be required to notify the ICO of:

a) all the trading names your organisation uses. If you have more than one organisation in a group then each will need to notify separately
b) name, work address and contact details of the data controller
c) a statement of security. This will not appear on the public register
d) a statement of any exempt processing if this applies.

12. Don't be misled

Some commercial organisations operate as data protection agents. They contact targeted companies stating that the company has not registered under the DPA and may be liable to prosecution. These companies offer to carry out the registration on your behalf usually in return for a fee. However, the process is straightforward and the Information Commissioner's office will help with the registration process to ensure that you get it right. Most organisations offering such services are genuine, although the Information Commissioner would like to be informed of any suspect approaches so action can be taken against these companies.

13. After notification - rights of access to personal data

Individuals (data subjects) have the right of access to their own personal data held by an organisation and to be informed of what it is being used for.

As a data controller, you can request the following from an individual wanting to see their data:

- sufficient information to verify the individual's identity
- for the request to be put into writing
- a charge of no more than £10

Individuals can then request:

- a description of the personal data that is being held
- the purposes for which this data is being held and processed
- details of whom they might be disclosed to.

Data subjects have the right to view all the information held by you about them; this includes emails, personal organisers, databases, CCTV records and copies of recorded phone conversations if relevant. A code of practice can be found on the ICO website. Once a request is received in writing from the data subject, the data controller has 40 calendar days to supply the information in an easily readable format. Failure to do so can result in prosecution. Third parties however, do not have the right to request details on the personal data held for another individual, unless the information is requested by an authorised body such as a law enforcement agency, HMRC or if a court order is provided. However, under certain circumstances, the Freedom of Information Act may mean that an individual's data can be requested by a third party, as for

example MPs' expenses, although this is limited to organisations operating in the public sector, not private companies.

The Information Commissioner's Office, the body responsible for enforcing the DPA, reviews complaints against data controllers or data processors breaking the rules. The ICO can serve information notices, requiring certain information to be supplied and enforcement notices requiring processing of personal data to be discontinued. If these requests are not met, penalties are leveled at the controllers or processors of the data; however directors or managers may be personally liable if breaches of the Act have occurred with their consent or through their neglect. Additionally, employees may be liable if they release or obtain information without the authority of a data controller.

Following a number of high profile cases of information loss, the ICO now requires that any data loss amounting to 1000 records or more, or anything deemed to be critical, be notified to them for investigation. Whilst typical fines of £500 per incident may not themselves be regarded as significant, the ICO publishes its decisions for public viewing on their website, so the adverse publicity, as well as the subsequent potential loss of business far outweighs any costs.

The ICO issued new guidelines in August 2013 to help organisations comply with subject access requests. This guidance aims to help organisations manage requests made under the DPA more efficiently as well as enabling members of the public to have greater control of the data held about them. The ICO has recently published a best practice code on the anonymisation of data to ensure that such data can be safely used without inadvertently breaching the DPA.

Managers should avoid:

- thinking that as you have the data in your possession you can sell it on to a third party. You do not own the data, the individual does, and without their consent you cannot do anything other than what you have told them in your Data Protection statement.
- thinking that you can transfer personal data across international borders as and when you want. If this has to be done however, it must be done in a compliant manner.

Glossary

Data subject	An identifiable living individual about whom data is kept
Data controller	The person in an organisation who directs how the data should be processed
Data processor	The person carrying out work on the data
Processing	The obtaining, recording and use of personal data
Notification	The process of registering a data controller's processing details with the Information Commissioner.

Standards and Related Guidance

Data Protection Act 1998
Electronic copies are available at www.legislation.gov.uk

BS ISO/IEC 27001:2013 (BS 7799-2:2013) Information technology. Security techniques. Information security management systems. Requirements

BS ISO/IEC 27002:2013 (BS 7799-1:2013) Information technology. Security techniques. Code of practice for information security management

BS 10012:2009 Data Protection – Specification for a personal information management system

BIP 0002 Data protection: Guidelines for the use of personal data in system testing, 2nd ed
London: BSI

National Occupational Standards for Management and Leadership

This checklist has relevance for the following standard:

Unit BB4 Ensure compliance with legal, regulatory, ethical and social requirements.
Unit EC2 Management information, knowledge and communication systems

Additional resources

Books

Data protection compliance in the UK: a pocket guide, 2nd ed. Jenna Clarke and Jay Rosemary
Ely: IT Governance Publishing, 2010
This title is also available as an e-book

BIP 0050:2009 Data Protection Pocket Guide: essential facts at your fingertips, 2nd ed. Nicola McKilligan and Naomi Powell
London: BSI, 2009

Data protection and compliance in context, Stewart Room
Swindon: British Computer Society, 2007

This is a selection of books available for loan to members from the Institute's library. More information at:
www.managers.org.uk/library

Internet resources

Guide to data protection
http://www.ico.gov.uk/for_organisations/data_protection_guide.aspx
A key resource identifying data protection basics; the role of the ICO; and key definitions.

CMI's data protection policy
www.managers.org.uk/dataprotection

Organisations

Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF
Helpline 0303 123 1113 Tel: 01625 545745 Fax: 01625 524510 Web: www.ico.gov.uk

British Standards Institution (BSI) 389 Chiswick High Rd, London, W4 4AL
Tel: 020 8996 9000 Fax: 020 8996 7400 Web: www.bsi-global.com

This is one of many checklists available to all CMI members. For more information please contact

t: 01536 204222 **e**: enquiries@managers.org.uk **w** www.managers.org.uk

Chartered Management Institute
Management House, Cottingham Road, Corby, NN17 1TT.

Revised Mar 2014