DATA PROTECTION ACT
Compliance self-help checklist

information commissioner
Barrantagh Fysseree

This self-help checklist is to assist you formulate a clear policy on data protection compliance.

It examines the issues in a structured manner in relation to compliance with the legal requirements of the Data Protection Act (DPA) and with the eight Data Protection Principles. The amount of detail you find useful will depend on the size of your organisation and the amount of personal information you hold.

If you can answer 'yes' to all these questions then your business is in good shape with regard to data protection. If not, it should help you pinpoint the areas that need improvement.

Compliance with the Legal Requirements

- ☐ Does the organisation need to register with the Information Commissioner?
  - o If so, is the register entry kept up to date?
  - o Does it accurately reflect our uses of personal information?
  - o Do we advise the Commissioner of any changes as soon as practicable?
- ☐ Does any individual, or role, within the organisation have responsibility for ensuring data protection compliance?
  - o Are staff aware of that person/role?
- ☐ Are there formal data protection compliance review mechanisms in place within the organisation?
- ☐ Are all staff aware of their responsibilities under the DPA?
- ☐ Is data protection included as part of the regular training programme for staff?
  - o Is a senior member of staff responsible for ensuring that training is provided and completed?

Compliance with the Eight Data Protection Principles

1. The First Principle: fair and lawful processing

Fair Processing

- ☐ Are our personal information collection processes open, transparent and up-front?
- ☐ Do we have a privacy notice or fair processing notice available for our clients?
  - ° Do we provide them with this at the time we collect their personal information?
  - ° Does it include details of any disclosures of their personal information to third parties?
- ☐ Have we obtained the client's consent for any secondary uses of their personal information that might not be obvious to them, e.g. direct marketing?

Purpose Specification

- Are we clear about the purpose(s) (reason) for which we use personal information?
- Are the clients also aware of the purpose(s)?
- Does our register entry include this purpose(s)?
- Does a person, or role, in the organisation have responsibility for maintaining a list of all information assets and their uses?

2. The Second Principle: purpose for which data are obtained and processed

- Are clients aware of the uses and disclosures of their data?
    - Would they be surprised if they learned about them?
- Do we have defined rules about the use and disclosure of personal information?
- Does our register entry, if required, include these uses and disclosures?

3. Third Principle: adequacy and relevance of data

- Do we only collect the information that is necessary for our specified purpose(s)?
- Can we justify the need to obtain and use each piece of information?
- Does a policy exist in this regard?

4. Fourth Principle: accuracy of data

- Do we check the accuracy of personal information when we collect it?
- Do we check the accuracy of personal information before we disclose it in some way?
- Do we keep our data up-to-date if needed?
    - Do we act quickly if a client advises us of any changes or inaccuracies in their personal information?

5. Fifth Principle: time for keeping data

- Do we know if there are any legal, or industry standard, retention periods that apply to the personal information the business holds and uses?
- Do we regularly remove personal information we no longer need?
- Is there a personal information retention and destruction policy?

6. Sixth Principle: rights of data subjects

The DPA contains many rights for individuals. The following are the most frequently exercised:

The Right of Access

- Can we recognise a subject access request?
- Is any individual, or role, within the organisation responsible for handling subject access requests?
- Are there clear procedures for dealing with such requests in accordance with the DPA?

The Right to object to Direct Marketing

- Do we give clients the right to object to direct marketing?
- Do we give clients the right to opt out with every electronic marketing communication?

7. Seventh Principle: measures against misuse and loss of data

- Does any individual, or role, within the organisation have overall responsibility for information security and ensuring that staff understand their responsibilities?
- Are there security measures in place to protect the personal information we hold and use?
    - Are these provisions appropriate to the sensitivity of the different types and uses of personal information?
- Are computers, servers, paper client files etc., secured from unauthorised physical access?
- If third parties process personal information on our behalf, do we have written agreements in place?
- Is there an information security/ information governance policy in place that staff are aware of and receive regular training in?
  Does this include:
    - The need for the use of password protection and/or encryption to current standards if necessary, particularly if personal information is emailed, taken off-site or portable devices are used?
    - Arrangements for the use of personally owned portable and mobile devices for work purposes either in the workplace or at home? (Bring Your Own Device)

8. Eighth Principle: transfer of data abroad

- Do we regularly transfer personal information to third countries?
    - If so, are we confident that there are appropriate security measures in place, and what steps do we take to check those measures?

Further guidance is available in the document library on the website.