
25 steps to data protection compliance

1 Introduction

Other parts have examined the scope and application of the DPA and have looked at some of the operations that involve personal data and the special considerations and responses that are appropriate to each data protection situation.

Each part provides advice on how to comply with the specific provisions of the DPA either in the body of the text or in high-level summary form as ‘action points’ which need to be read and acted on together.

This part is designed simply to summarize the framework, and the general strategy within which the action points and advice contained in the individual parts should be carried out. It provides an overview of the situation confronting managers, and outlines steps that should be taken in designing a general strategy to comply with the DPA and its requirements and to translate it into operations as effectively and fluently as possible. The demands and requirements of the law will obviously condition some of these steps; others will simply be good practice, whatever the circumstances.

The emphasis is on taking responsibility for personal data and the need to aim for efficient, thorough and secure management of activity in this area.

It should be noted that the existence of an action plan does not suggest the adoption of a ‘once and for all’ approach to data protection management. Practices should evolve seamlessly into an ongoing active data protection regime.

2 Management action – 25 steps to data protection compliance

2.1 Appoint a data protection coordinator

1. Appoint a person tasked with responsibility for managing data protection compliance if you do not already have one. (A larger organization may consider assembling a team to deal with the implementation.)

2.2 Develop and implement a data protection strategy

2. Develop and disseminate an approved data protection policy.
3. Develop a data protection strategic plan and an operational specification to implement policy.
4. Estimate the resources that you will need to manage, and to continue managing, data protection.

2.3 Develop and implement awareness, education and training strategies

5. Maintain current awareness of developments in data protection. (Pay particular attention to developments in the law and any output from the Information Commissioner’s Office, as well as any from your trade/professional association.)
6. Amend staff conditions of service to include information about their rights and their obligations regarding personal data.

7. Ensure that staff are being adequately trained and instructed – this will entail regular updating sessions as well as induction together with properly documented working instructions.
8. Ensure that adequate information is being circulated about data protection in general and the way in which you are implementing it.

2.4 Develop and implement audit and documentation policies

9. Establish the nature and extent of all current personal data processing by conducting a thorough audit of:
 - manual data;
 - automated data.

Remember processing will include:

- a) where you get information from;
- b) what you do with it;
- c) why, where, and to whom it is given;
- d) how you look after it;
- e) how you dispose of it (in accordance with your retention policy).

10. Document the results of the audit appropriately so that:
 - a) information for checking the accuracy of your notification to the Information Commissioner is readily available;
 - b) those responsible for personal information internally can be contacted to verify their activity;
 - c) information about the use of personal data throughout the organization can easily be collated – for example:
 - information about similar purposes and uses of information;
 - information about similar types of data subject.

Do not forget outlying branches and departments. Do not forget about personal data that your employees are holding and using on their laptops or home PCs (whether or not with your authority). Do not forget data that is being processed on your behalf by your data processors.

NOTE Guidance on conducting a data protection audit is given in ‘Assessment of compliance’ (online).

11. Decide which of your manual systems for handling personal data fall under the scope of the DPA.
12. Reassess the need for all current personal data processing and eliminate any that is not necessary, or can be achieved by alternative means.
13. Reassess your routine office operations; pay particular attention to security, supervision, efficiency and accuracy and make improvements where necessary. Remember that manual records will need appropriate attention.
14. Make an occasional spot check of your personal data-handling activity to make sure that it is being done properly. Do this for both automated and manual information.
15. Test your capability to respond to a breakdown and other serious contingencies in your operations, quickly, completely and efficiently, as it affects personal data handling and data protection (disaster recovery planning). Do this for both automated and manual information.

16. Consult and follow any authorized Codes of Practice that have been issued for your sector of activity.
17. Maintain the quality of data protection management through a regular review mechanism.

2.5 Review and maintain your notifications

18. Review your existing data protection registration for completeness and accuracy and review its applicability. Make any amendments and deletions to the registration that are appropriate.
19. Notify the Information Commissioner about new processing and any renewals of existing processing that may be necessary.

2.6 Develop and implement policies and procedures to deliver subjects' rights

20. Review your current arrangements for providing data subjects with information and responding to any complaints about information under the DPA, and make any improvements that are appropriate. Note that these arrangements need to be extended appropriately to manual personal data.
21. Notify data subjects about processing that involves them that may be necessary. Remember that this will include manual personal data. Regard this not simply as a legal obligation but as an opportunity to reassure clients, suppliers and staff that you are managing well.
22. Seek formal informed consent from data subjects about the processing of any sensitive data (as defined by the DPA) that involves them. Remember that this will include manual personal data.
23. Arrange, with respect to manual information, to provide data subjects with information and respond to any complaints about information under the DPA.

2.7 Enter into contracts with third-party processors

24. Enter into contracts with any data processors that undertake work for you and ensure that strict quality, security and data protection compliance mechanisms and inspection procedures are agreed with them. Remember that those who process manual information (such as microfilming your records, or paper disposal) as well as those who undertake automated data processing will need to be included.

2.8 Develop a disaster recovery plan

25. Review your ability to respond to a data subject access request quickly, completely and efficiently, even during or after an incident. Do this for both automated and manual information.

3 End note

The array of steps to good practice outlined here are necessarily simplified and are not a comprehensive blueprint of data protection management. They will serve as a framework upon which to plan the implementation of data protection successfully. Local circumstances and preferences will condition which aspects are developed fully and what detail will be included. The manager on the spot is best placed to determine the precise strategy and practices to follow, and he/she should do so with confidence. The brief steps outlined here should be considered in parallel with the more detailed guidance in Part 1, 'How to comply with the DPA'.