

DATA PROTECTION AUDIT QUESTIONNAIRE

1. Purpose

The purpose of a data protection audit is to obtain a complete picture, as far as possible, of the structure of personal information flows within an organisation so that the appropriate compliance procedures can be put in place to ensure that the organisation deals with personal data in accordance with data protection law, the general law and best practices.

2. Organisation Chart

For large-scale and complex organisations the first stage is to obtain an organisational chart showing the operational, managerial and departmental structure of the organisation together with the names and locations of the personnel who have managerial or operational responsibility for information within the organisation.

3. Questionnaires

Data protection audit questionnaires should then be sent to each named individual for completion or may be used as the basis for face to face interviews.

4. Analysis of information

Once all the questionnaires have been completed the organisation is in a position to compile a complete diagram of the use of information within the organisation which can then form the basis of a review of the organisation's compliance with data protection law and other relevant law.

For large-scale and complex organizations, it is recommended that such audits are carried out annually.

5. The Data Protection Audit Questionnaire

Name:

Job Title:

Department:

Address:

Collection

1. Does your department process personal data on:

Individuals:-

Sole traders:-

Partnerships:-

Companies:-

Other public or private organisations, institutions, bodies, etc:-

2. If so, who authorises the collection?

.....

.....

3. For what purposes are the information collected?

.....

.....

.....

.....

.....

4. What information is collected?

.....

.....

.....

.....

.....

5. How is the information collected? Is it collected face to face with the individual or at a distance?

If face to face, is collection:

by interview:-

in a retail outlet:-

by attendance at an event or of function:-

or by other means:-

If collection occurs at a distance, is it:

an in-bound telephone call:-

an out-bound telephone call:-

via the Internet website:-

a fax:-

or by other means:-

In either case, is a paper format used such as an application form or any other method of compiling such information? Please attach examples.

.....
.....

6. From whom is the personal data collected:

individuals themselves:-

third parties:-

intermediaries, e.g list brokers:-

financial advisers, joint venture partners, etc:-

7. What form of data protection notice is given to individuals when the information is collected? Please attach copies.

.....

.....

8. How often is this notice reviewed or changed?

.....

.....

9. Who reviews or changes the notice?

.....

.....

Storage, Processing and Disclosure

10. Does your department store personal information? If so, is the storage:

on computer:-

in manual files:-

both on computer and manually:-

11. If storage of information is on computer, is this:

in-house:-

by third parties:-

12. If storage is on computer, where is it located?

.....

.....

13. What processing activities are carried out by your department?

.....

.....

14. Are any of your processing activities carried out by third parties? If so, please list them and describe the processes.

.....

.....

15. Who authorises these processing activities?

.....

.....

16. Who has authority to change, add or delete data?

.....

.....

17. Who has access to personal data? Please list?

within the organisation:-

outside the organisation:-

18. Who authorises such access?

.....
.....

19. Describe the manual filing storage system?

.....
.....

20. Do you consider that your department holds any sensitive data? If so, please describe the sensitive data and why it is held.

.....
.....

21. Do you disclose data to:

Other departments in the organisation:-

Third parties outside the organisation:-

22. In what countries are those people to whom you disclose the information (whether inside the organisation or external) located? Please list.

.....

Subject access procedures

23. Please describe the procedures in your department for supplying information in response to a data subject access to personal data request?

.....

.....

24. What procedures exist in your department for suppression, blocking or correction of personal information?

.....

.....

25. Who authorises these activities?

.....

.....

Data quality

26. Who in your department has responsibility for reviewing personal data for relevance, accuracy and keeping personal data up to date? How often are these activities carried out?

.....

.....

Security

27. Describe in outline the security procedures in operation in your department to keep all information secure. Please describe the physical, logical and technological procedures used?

.....

.....

Destruction or archiving

28. How long is personal information kept in your department before being destroyed or archived?

.....

.....

29. Who authorises destruction?

.....

.....

30. Who authorises archiving?

.....

.....

31. Please describe the archiving procedures in operation in your department?

.....

.....

32. Please give the location of your department's archived information?

.....

.....

33. In what format or on what medium is the archived information stored?

.....

.....

Training

34. Do the employees in your department receive training on data protection law and other relevant law? If so, who is responsible for carrying out the training?

.....

.....

35. Are refresher courses held? If so, how often and who is directed to attend?

.....

.....

Future Business Requirements

36. Do you foresee in the next twelve months a change in any of the answers you have given? If so, please describe the changes.

.....

.....