Data Protection Act 1998 - Principles of Compliance

First Principle

"***Personal data shall be processed fairly and lawfully.***"

Second Principle

"*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".*

Third Principle

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

Fourth Principle

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

Fifth Principle

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

Sixth Principle

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

Seventh Principle

"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".

Eighth Principle

"*Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection of the rights and freedoms of data subjects in relation to the processing of personal data".*

Data Protection Act

The Data Protection Act 1998 (the "Act"), together with a number of Statutory Instruments (a list of which appears in the annex to this publication) came into force on 1 March 2000, repealing the Data Protection Act 1984.

The Freedom of Information Act 2000 (the "FoIA") received Royal Assent on 30 November 2000. Some of its provisions came into force on or after 30 January 2001.

This Law needs greater attention as it covers a potential multitude of sins. It is necessary here to quote the introduction and convey the message to administrators. Policies on Access control and data storage should provide the protection required but especial recognition of the organisations (here called data collectors) obligations to data owners (here referred to as data subjects).

"All data controllers are under a duty to comply with the Data Protection Principles in relation to all personal data with respect to which they are the data controller (subject to the various exemptions). Some manual data are now also included within this definition. Non-automated information may be found in a variety of different media e.g. paper files, rollerdex, non-automated microfiches. Data controllers should examine all their non-automated information systems (referred to in this chapter as "manual information") in order to determine how far the Act applies to personal data processed in those systems. To be subject to the Act, the manual information must fall within the definition of "data" in the Act. As indicated at paragraph 2.1(c) above, data includes information which is recorded as part of a "relevant filing system" or with the intention that it should form part of a "relevant filing system". The term "relevant filing system" means:-

"any set of information relating to individuals to the extent that, although the information is not processed by means of equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible"

Below I briefly set out the eight principles to demonstrate that BS7799 Part 1, first nine guidelines are insufficient in themselves to merit compliance. It should be repeated and stressed that the full Act should be read and discussed with the legal department and in the case of financial organisations and credit companies deference to the accreditors of FIS is mandatory. Similar concentration should be given to Data Protection Law in other countries.

Principles of Compliance

First Principle

"Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless

- at least one of the conditions in Schedule 2 is met; and
- in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met."

Parts of Schedule 2 and 3 are contained in Annex A. However Meeting a Schedule 2 and Schedule 3 condition will not, on its own, guarantee that processing is fair and lawful. The general requirement that data be processed fairly and lawfully must be satisfied in addition to meeting the conditions.

In particular the organisation must look at the sentiment behind the first principle which ***is not automatically followed just through the application of all the earlier ISO 27001 Annex A controls.***

.

> Even though a data controller may be able to show that information was obtained and personal data processed fairly and lawfully in general and on most occasions, if it has been obtained unfairly in relation to one individual there will have been a contravention of the First Principle.
>
> Automated processing can be unfair either where the program is itself operating correctly, but results in the unfair use of data, or where a program is of poor quality and contains errors which mean that it does not operate as the data controller intended.

Compliance with the fair processing requirements of the Act provides an opportunity for data controllers to obtain consent (as to which, see above) but such compliance will not, in itself, ensure that any purported consent is both "specific" and "informed". It is most important to the assessor of BS7799 that the organisation processing data has procedures in place to ensure that data subjects i.e. the "owners" of data are informed of the data retention and can gain knowledge of personal data held and ensure its accuracy and relevance. Timeliness and appropriate effort in disclosure are important factors to be considered when assessing the procedures.

Second Principle

"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".

The interpretation of the Second Principle further provides that in deciding whether any disclosure of personal data is compatible with the purpose or purposes for which the data were obtained, consideration will be given to the purpose or purposes for which the personal data are intended to be processed by any person to whom they are disclosed. Such decisions cannot be made retrospectively by data controllers once the data are obtained. For the purposes of the Second Principle, the further processing of personal data in compliance with the conditions set out in section 33 of the Act is not to be regarded as incompatible with the purposes for which they were obtained. Adherence to paragraph I of Part II of Schedule I is clearly material in this context in that data subjects must not be deceived or misled as to the purposes for which their personal data are to be processed.

Third Principle

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

In complying with this Principle, data controllers should seek to identify the minimum amount of information that is required in order properly to fulfil their purpose and this will be a question of fact in each case. If it is necessary to hold additional information about certain individuals, such information should only be collected and recorded in

those cases. It is not acceptable to hold information on the basis that it might possibly be useful in the future without a view of how it will be used. This is to be distinguished from holding information in the case of a particular foreseeable contingency which may never occur, for example, where an employer holds details of blood groups of employees engaged in hazardous occupations. Data controllers should continually monitor compliance with this Principle, which has obvious links with the Fourth and Fifth Principles. Changes in circumstances or failure to keep the information up to date may mean that information that was originally adequate becomes inadequate. If the data are kept for longer than necessary then they may well be both irrelevant and excessive. In most cases, data controllers should be able to remedy possible breaches of the Principle by the erasure or addition of particular items of personal data so that the information is no longer excessive, inadequate, or irrelevant. Procedures should exist to record for all data:

- the number of individuals on whom information is held;
- the number of individuals for whom it is used;
- the nature of the personal data;
- the length of time it is held;
- the way it was obtained;
- the possible consequences for individuals of the holding or erasure of the data;
- the way in which it is used;
- the purpose for which it is held.

Fourth Principle

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

The Organisation must have procedures in place to ensure that its databases are accurate. Data is inaccurate if it is incorrect or misleading as to any matter of fact. The Act provides guidance in interpreting this Principle as follows: The Principle is not to be taken as being contravened because of any inaccuracy in personal data which accurately record information obtained by the data controller from the data subject or a third party in a case where:

(a) taking account of the purpose or purposes for which the data were obtained and further processed, the data controller has taken reasonable steps to ensure the accuracy of the data, **and**

(b) if the data subject has notified the data controller of the data subject's view that the data are inaccurate, the data indicate that fact.

It is important to note that by virtue of (a) above it is not enough for a data controller to say that, because the information was obtained from either the data subject or a third party, they had done all that they could reasonably have done to ensure the accuracy of the data at the time. Now data controllers may have to go further and take reasonable steps to ensure the accuracy of the data themselves and mark the data with any objections. The extent to which such steps are necessary will be a matter of fact in each individual case and will depend upon the nature of the data and the consequences of the inaccuracy for the data subject. This approach exceeds the requirements of the Fifth Principle in the 1984 Act.

The second part of the Principle, which refers to keeping personal data up to date, is qualified. Updating is only required "where necessary". The purpose for which the data are held or used will be relevant in deciding whether updating is necessary. For example, if the data are intended to be used merely as an historical record of a transaction between the data controller and the data subject, updating would be inappropriate. To change the data so as to bring them up to date would defeat the purpose of maintaining the historical record. However, sometimes it is important for the purpose that the data reflect the data subject's current circumstances, for example, if the data are used to decide whether to grant credit or confer or withhold some other benefit. In those cases either steps should be taken to ensure that the data are kept up to date, or when the data are used, account should be taken of the fact that circumstances may have changed. The assessor must ensure that processes are in place to ensure:

- Is there a record of when the data were recorded or last updated?
- That if the personal data is possibly out of date, all those involved with the data – including people to whom they are disclosed as well as employees of the data controller – are aware that the data do not necessarily reflect the current position?
- Steps taken to update the personal data – for example, by checking back at intervals with the original source or with the data subject? If so, how effective are these steps?
- That if the personal data is out of date, it is unlikely to cause damage or distress to the data subject.

Fifth Principle

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

To comply with this Principle, the organisation should have written procedures to review their personal data regularly and to delete the information which is no longer required for their purposes. Statutes may make specific provision relating to the retention of certain categories of data, for example, the Police and Criminal Evidence Act 1984. Recommendations with regard to the retention of certain information can be found in the CCTV Code of Practice published by the Commissioner which contains guidance on the retention periods of recorded material. If personal data has been recorded because of a relationship between the data controller and the data subject, the need to keep the information should be considered when the relationship ceases to exist. For example, the data subject may be an employee who has left the employment of the data controller. The end of the relationship will not necessarily cause the data controller to delete all the personal data. It may well be necessary to keep some of the information so that the data controller will be able to confirm details of the data subject 's employment for, say, the provision of references in the future or to enable the employer to provide the relevant information in respect of the data subject's pension arrangements. It may well be necessary in some cases to retain certain information to enable the data controller to defend legal claims, which may be made in the future. Unless there is some other reason for keeping them, the personal data should be deleted when the possibility of a claim arising no longer exists i.e when the relevant statutory time limit has expired. The data controller may wish to consider the value of records for historical purposes. The Act provides that personal data processed only for historical, statistical or research purposes may be kept indefinitely.

Sixth Principle

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

The organisation should declare their intention to notify data subjects of their intent to process data and generally comply with the first five principles.

Seventh Principle

"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".

As noted before, compliance with the first six principles of the ACT together with appropriate compliance with BS7799 guidelines 1 thru 9 is likely to allow conformity to the Seventh Principle. However note that remedial action may be needed to ensure that, with regard to the technical and organisational measures to be taken by data controllers, that such measures should be taken " both at the time of the design of the processing system and at the time of the processing itself."

Eighth Principle

"*Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection of the rights and freedoms of data subjects in relation to the processing of personal data".*

Compliance with this principle should be evident in company procedures. The European Economic Area ("The EEA") consists of the fifteen EU Member States together with Iceland, Liechtenstein and Norway. The EU has defined privacy laws that in general are more prescriptive that those applied in the USA. Therefore the transfer of personal information from the EU to the United States when equivalent personal protections are not in place in the United States is prohibited. I once worked for a credit card company, actually the third largest in the USA, whose UK arm wished to avail itself of the latest fraud detection software house, housed in Texas. Strict guidelines had to be complied with before the FIS let such transfers of data take place.

The interpretation to the Eighth Principle provides that an adequate level of protection is one which is adequate in all the circumstances of the case, having regard in particular to:

- the nature of the personal data,
- the country or territory of origin of the information contained in the data,
- the country or territory of final destination of that information,
- the purposes for which and period during which the data are intended to be processed,
- the law in force in the country or territory in question,
- the international obligations of that country or territory,
- any relevant codes of conduct or other rules which are enforceable in that country or territory (whether generally or by arrangement in particular cases), and

- any security measures taken in respect of the data in that country or territory

Note that there are all sorts of caveats that allow transfer, relating to the permissions of the owner and the necessity of the transfer. For the auditor it is necessary only to ensure the Principle is being adequately addressed not that the interpretation of the law in individual circumstances is absolute. If in doubt consult the organisations legal department.