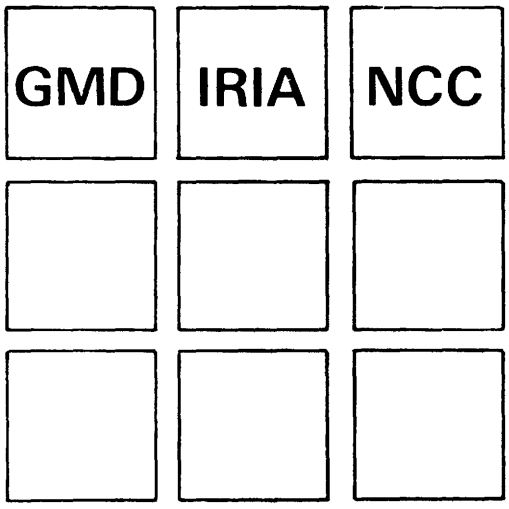


STUDY ON

DATA SECURITY AND CONFIDENTIALITY

FINAL REPORT

to the Commission for the European Communities

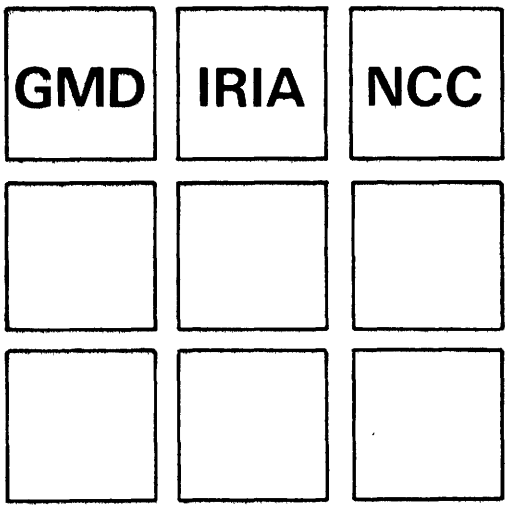
Volume 6 of 6

Section 6: Data protection inspection

by H H W Pitcher

Section 7: Conclusion

JANUARY 1980



STUDY ON

DATA SECURITY AND CONFIDENTIALITY

FINAL REPORT

to the Commission for the European Communities

Volume 6 of 6

Section 6: Data protection inspection

by H H W Pitcher

Section 7: Conclusion

JANUARY 1980

Contents of all volumes

Contents of section 6

6 Data protection inspection

6.0 Introduction

6.0.1 The motivation for this item

There are already data protection laws in serveral countries, and many more are expected in the next few years. But laws in themselves, though they may deter, do not prevent abuses: "Many people in the industry feel that the only people they (data protection regulations) will affect are the honest; anyone who is determined in evade them will succeed."

(J1). It was understandable that initially the main interest should be in recognising the existence of troubles arising in the use of personal data, and their causes, and in developing means of avoiding them; but the time comes when thought must be given to the enforcement of the laws.

The implies some means of checking whether people are complying with the laws: "Without proper inspection and supervision, the unscrupulous will always misuse any situation."

I1:qn.2). Some data laws recognise this need, eg the Swedish Data Inspection Board can demand access to premises, computers, documents and other information (S1: sections 16, 17, 24). However, relatively little has been published about such inspection for data protection enforcement, and there is considerable uncertainty about how it could be done. Indeed, it has been argued (J1) that it is impossible, without the co-operation of the person who operates it, to check whether a system satisfies a data protection law; and therefore at the whole idea of data protection regulation by law is unsound.

Such uncertainty and scepticism deserve answers, and it is the purpose of section 6 to explore the whole question of the envisaged inspections with a view to at least narrowing the area of ignorance concerning them.

6.0.2 The purposes of inspection

The prime objective of the inspection is simply to check to what extent a particular system containing personal data complies with the appropriate data protection regulations. However, several other benefits will follow:

1. The data user will learn where his system needs improvement in the name of data protection.

2. Evidence will be provided for prosecution of non-complicance.

3. If there were an effective method of enforcement, data subjects could have more confidence that their complaints of data abuse would b effectively pursued.

4. Data users generally will be encouraged to comply with data protection regulations; standards of performance in data protection will be progressively improved.

5. The general standard of performance in data protection will be monitored, which will give evidence to reassure or alert the public.

6.0.3 Structure of section 6

The structure of the rest of section 6 is as follows. Insection 6.1 the special meaning with which particular terms are used throughout section 6 is explained. Section 6.2 deals with some issues which must be considered before the inspection procedure can be readily understood or discussed. In section 6.3 the essential principles of data protection are expanded into a set of measures which data users may be expected to follow.

The following sections 6.4 to 6.6 expound the actual inspection procedures for checking that these measures are being followed. Section 6.7 discusses questions particularly related to the person of the inspector, section 6.8. discusses various further questions which relate to the inspection procedure, and finally section 6.9 lists materials referred to or used in section 6.

6.0.4 Referencing system

The following system of referencing is used. Cross references to sections of this report are given by the number of the section referred to. References to the bibliography consist of a capital letter followed by a number; this may be followed by a colon and a reference using the reference system of the document referred to. Thus "H1:p.xx" refers to page number xx of the United States HEW report.

6.1 Definitions

6.1.0 Introduction

Section 6.1 contains explanations of some terms which are used throughout Section 6 with particular meanings. To facilitate understanding, a brief description of the inspection will now be given, showing the context in which the terms arise. The terms are here underlined.

An organisation will often hold personal data which is used in several systems by one or more data users. This date refers to data subjects and may be covered by legal or other regulations. To check whether a system complies with the regulations, a commissioning body (which may or may not be the legally-appointed Authority), may order an inspection to be carried out by the inspector, who makes an inspection visit, collects information and produces an inspection report.

6.1.1 Definition of 'organisation'

The term 'organisation' is used to refer to the body which runs the system which is being inspected. The organisation is regarded as being practically responsible for the system, is expected to be able to answer all questions about it, and to give the inspector the practical powers he needs.

In simple cases the organisation will be a company or other well-defined body, and will have total legal responsibility for the system. But the use of complicated systems may be shared by several companies, and small systems may be in practice out of control of the nominally responsible body, e.g. a student's research file may not be know by the host university. In such cases the inspector may have difficulty in collecting the information which he needs.

The organisation should not be conceived necessarily as an ordinary commercial firm. A large proportion of personal data handling occurs in such sectors as central and local government, public utilities, and charities, and the leisure use of computers is increasing fast. The significance of this for inspection is that the motivation for breach of the regulations will not always be financial (cf.6.2.2).

6.1.2 Definition of 'system'

Throughout section 6, the term 'system' is used to refer to the totality which is the subject of the inspection. The term could apply to objects of very different types. For example, each of the following could be treated as a system for the purpose of inspection:

1. The payroll operations of a single organisation.
2. All the data processing activities which involve personal data within one organisation. It may be more efficient to inspect these together rather than separately, though they are in no sense a unified system.
3. The SWIFT network, which links 500 banks in 15 different countries (1.1.2.2).

Each of these is a system in the sense that it has boundaries which are conceptually clear within which personal data is handled in a way which one might wish to inspect. It will become clear that the principles of inspection are similar for all systems.

Although the main emphasis in data protection legislation has been on computerised systems, the proposed method of inspection is also applicable to systems which do not contain a computer.

6.1.3 Definition of 'data user'

The term 'data user' is used to refer to the person or persons who in practice make decisions about the system. He will normally be only a small part of the 'organisation', and may or may not be legally responsible. From the inspector's point of view, the 'data user' is a part of the organisation which he must mostly look to for answers.

In much of section 6, the distinction between the roles of the organisation and the data user is not essential.

6.1.4 Definition of 'data', 'data subject', 'information'

Throughout section 6, 'data' usually means 'personal data', and the precise meaning to be given to that expression will depend on the regulations. The trend in data protection is towards embracing any data which relates to an identified person. To save the word 'data' for this restricted meaning, the word 'information' is used in this section to refer to such things as particulars of the system.

The terms 'data subject' is used here in what is becoming its standard meaning, viz. a person to whom personal data refers. The distinction between a physical person and a non-physical person (section 3) is almost immaterial for inspection purposes (although of course the inspector must know what sort of person is covered by the regulations). It must not be assumed that the data subject is the best person to look after his interests: the precedent of a child having a legal guardian shows this.

6.1.5 Definition of 'regulations'

The main purpose of inspection (6.0.2) is to check the extent to which some particular set of rules relating to

personal data is being obeyed. This set of rules is here termed the 'regulations'. It is not necessary that they have the force of law, or be derived from the law: they may be wider or narrower than this, at the discretion of the commissioning body. For example, in a voluntary inspection it may be convenient to cover only one aspect of the law during a particular inspection, inspection with regard to the other aspects being postponed; or, in following up a specific complaint, a statutory inspection may be concerned primarily with the apparently delinquent parts of the system. However, the regulations must be practically limited to data protection requirements, else the scope of the inspection could be impossibly wide.

The regulations must be applicable to the system, and must be precise enough for compliance with them to be testable. It is not the inspector's role to use his judgement to covert ambiguous regulations into specific requirements: for this he should refer to the commissioning body.

6.1.6 Definition of 'commissioning body', 'Authority'

It is the commissioning body which initiates the inspection, determines its scope, chooses the inspector, gives him whatever powers he possesses, receives his report and decides on any such subsequent action. In some circumstances, the regulations may not be identical to the law, as explained in the previous section (6.1.5);

it is the commissioning body which determines the regulations which are to be the basis for the inspection. The inspector is totally subordinate to the commissioning body (subject to any citizen's obligations under the law).

Under some data protection laws, there is a central body which has legal responsibilities and powers (among other things) to initiate inspections to check compliance with the law. This body is here termed the Authority.

For a statutory inspection, the commissioning body is the Authority; for a voluntary inspection, some department of the organisation.

6.1.7 Definition of 'inspection', 'inspection visit', 'inspection report'

The word 'inspection' is used in two senses in section 6. Generally, it is used to refer to the whole art, science and discipline of checking compliance with data protection legislations, including (as will be seen in sections 6.2 and 6.8) many peripheral issues. More particularly, 'an inspection' is used to refer to a case of carrying out this checking, beginning with a decision to inspect and ending when the inspection report is received by the commissioning body.

As part of an inspection, it will usually be necessary for the inspector to go to the places where the system is operated, to see the system in operation and to interview the people involved. This is what is termed the inspection visit, without implying anything about the length of time or the number of comings and goings which are required.

The immediate result of an inspection will be the inspection report, in which the inspector presents his findings. The contents of this are discussed below (6.6.2).

6.1.8 Definition of 'inspector'

The term 'inspector' is used throughout section 6 to refer to the person or persons who carry out an inspection; the question of whether more than one person is needed is considered later (6.7.2).

6.2 Preliminary questions

6.2.0 Introduction

In section 6.2 several matters are discussed which must be understood before the inspection itself can be treated. Matters which can be postponed are placed in 6.8.

6.2.1 Actual and potential breaches

The regulations may be so specific, and the inspection so thorough, that the inspector can report directly on the degree to which the system complies with the regulations. However, this will rarely be the whole story. It is more likely that the regulations will set out objectives, the achievement of which requires various measures. If these measures are not carried out, this may not itself be a breach of the regulations, but it is a weakness of the system which constitutes a risk that a breach will occur. The inspector should normally direct most of his effort towards such potential breaches.

An example may make this clear. The regulations may say that the data must be accurate. For most systems this is an impracticable ideal, and therefore legally unenforceable. However, the data user will be required to closely approach the ideal, and to do this must take

suitable measures, such as using reliable data sources and data preparation methods, and checking the accuracy of the stored data. In turn, the inspector might check the accuracy of the stored data, and if he found too many inaccuracies he would report an actual breach of the regulations. Alternatively or in addition, he might check that the above-mentioned suitable measures have been instituted and are correctly carried out. If they are not, he would report the fact as a potential breach of the regulations.

The reason for this is that, if there are too many potential breaches, there is a high probability that there will sooner or later be actual breaches. The former are in most cases much easier to detect than the latter, and are therefore a more cost-effective area for inspection. This may present a conceptual difficulty in some data users, who may find themselves criticised when they think they have actually done nothing wrong.

If the data user is to be prosecuted under the law which requires evidence of an actual breach, the inspector must look for it. The potential breaches will be a good starting place for his search.

6.2.2 Selection of inspection areas

Although the inspector is in principle interested in all possible forms of non-compliance and all methods of

detecting them, pressures of economy will tend to restrict him to a small part of the whole. A means of making a reasonable selection of inspection measures is provided by the concepts of risk analysis, a process which, as part of risk management, has been developed from insurance management (P2,W2).

Broadly speaking, risk analysis involves the identification of possible breaches of the regulations and then estimating the importance of each possible breach. The importance of a possible breach depends on the following factors:

1. The underlying reasons or pressure for the breach. The reasons covers everything which might cause someone to commit a breach and includes:
   - financial gain
   - inquisitiveness
   - laziness
   - ignorance
   - incompetence
   - administrative zeal
   - criminal purposes, e.g. for blackmail
   - coercion by others
   - intellectual challenge
   - acquisition of information with which to please or impress others
   - hunger for power.

2. The opportunity for occurrence of the breach. This would involve an assessment of the ease of committing the breach, and the effectiveness of the relevant counter measures.
3 The seriousness of the consequences of the breach.

One could attempt to quantify the 'pressure', the 'opportunity' and the 'seriousness', and, by multiplying the three values, obtain a numerical weight to express the importance of each possible breach. However, the accuracy with which these variables can be estimated will rarely give much confidence in the result. It is probably better to use the approach to reveal what are qualitatively the most important potential dangers of the system.

The choice of inspection measures to be employed in a particular inspection should be influenced by two other factors:

- their expected effectiveness in disclosing the type of breach under consideration
- their estimated cost (including both personnel and computer time) to apply.

As with the analysis of the consequences of the breach, the value of this approach to inspection comes more from the concentration of thought on aspects which are relatively worthwhile than from attempts to ascribe numerical values to these factors.

6.2.3 The powers of the inspector

To carry out the inspection, the inspector may need these powers:

1. To obtain answers to questions.
2. To see and make temporary copies of documents and files.
3. To speak to people in private.
4. To inspect buildings and equipment.
5. To carry out computer runs using the hardware, programs and data used by the system.
6. To contact data subjects.
7. To use temporary working accommodation and facilities within the organisation.

The inspector derives his powers from the commissioning body, and if he finds that they are frustrated it is to that body which he must look. If his powers remain insufficient for him to carry out parts of his inspection, he should say so in his report to the commissioning body. It is not the inspector's job to decide what powers he is entitled to have, and he should recognise that there are legitimate reasons why they may be limited.

6.2.4 Statutory and Voluntary Inspections

Two different types of inspection are envisaged. It is convenient to display their differences in parallel:

Statutory inspection	Voluntary inspection
The statutory inspection may be required by law.	The voluntary inspection is not required by law.
Its immediate purpose is to detect non-compliance with the data protection law.	Its purpose is to check, for the benefit of the organisation, the degree of compliance of the system with the data protection law.
It is initiated by the Authority, which (subject to the law) determines its timing (perhaps in consultation with the date user), scope and stringency.	It is initiated by the organisation, which determines its timing, scope and stringency.
If a serious breach of law is found, the consequences for the system and its user may be catastrophic.	If serious faults are found, drastic action may be needed, but on a time scale determined by the organisation.
The inspector must be acceptable to the Authority.	The inspector is appointed by the organisation.

In case of difficulty, he can appeal to the Authority for whatever powers (within the law) he needs to carry out the inspection.	His powers will be determined by the organisation, and can be extended or curtailed at any time.
Statutory inspections will occur when the Authority considers them necessary.	Voluntary inspections occur at the convenience of the organisation.

Despite these differences, most aspects of inspection are similar, and it turns out to be unnecessary to distinguish the two types in most of the following discussion.

6.2.5 An inspection paradox

It is often said that any inspection procedure can be defeated. It is also asserted that any abuse can in principle be detected. These statements can be reconciled by accepting that any fixed object (inspection procedure/system of data abuse) can be bypassed by a moveable object (system or data abuse/inspection procedure). The moral for inspectors is that they must not become set in rigid inspection procedures, but must vary them, and improve them as experience accumulates and technology advances.

The subsidiary purposes of data inspection (6.0.2) do not depend on one hundred percent success by the inspector, and nor does law enforcement in general.

6.2.6 Strictness

The word 'strictness' is used with reference to at least three different aspects in this subject, and it may help reduce confusion to discuss them briefly:

1. Strictness of regulations means the extent to which the regulations impose burdens and limitations upon the data user. For example, a regulation requiring answering within one week a data subject's demand for a copy of the data which refers to him is stricter than one requiring answering within one month, and both are stricter than one requiring answering without specifying a time limit. To some extent strictness and preciseness to together, for example, a regulation saying that data must be 'accurate' is too imprecise to be regarded as strict (unless it is known that it will be interpreted in a particular way, in which case it is the implicit regulations which are strict).

2. Strictness of compliance refers to the closeness with which the data user satisfies the regulations. In essence, it is this which the inspection is concerned to assess. If the regulations are imprecise, there may be a large element of judgement in assessing the degree of compliance.

3. Strictness of inspection refers to the thoroughness of the inspection procedure, that is the confidence one can have that its assessment of the degree of compliance is accurate. The main aim of Section 6 is to specify an inspection procedure which can be as strict as will ever by necessary, but it is expected that the full rigour will very rarely be used. This question is discussed further in 6.8.2.

6.2.7 Global uniformity

There are several factors which may influence the inspection procedure:

1. The content of the regulations. The data protection laws of different countries differ considerably in their scope, precision and style.

2. The hardware of the inspected system, which might be anything between a pocket-sized notebook and a world-wide communications network.

3. The desired strictness (6.2.6) of the inspection

4. The social, political and ethical environment of the system, e.g. the tradition of complying with or evading laws, the tendency to co-opeate with Authority.

If it proved necessary to devise a correspondingly wide range of inspection procedures to suit all these possibilities, the whole subject would be unsatisfactory. It is here contended that this is not necessary: the inspection procedure which is offered provides a suitable framework for any data protection inspection, and nearly all the material that would be needed. The only substantial changes which might be needed are the omission of those parts which are not required by the particular regulations, or because of the hardware of the system, and a relaxation of the thoroughness of the inspection in appropriate circumstances.

The main reason for this is that the principles which underlie all data protection regulations can be related directly to a series of aspects of the system which are amenable to inspection, as is shown mostly in sections 6.3 and 6.5.

6.3 The principles of data protection

6.3.0 Introduction

In section 6.3 the few essential principles of data protection are discussed and related to several formulations in the literature. From them flow the regulations (6.1.5) and from these the requirements that the inspection must check (see especially 6.5).

Following the Lindop report (L1:1.11), the view taken here is that data protection should not be regarded as simply a battle between data user and data subject. There is a third interested party (society at large), and the purpose of data protection is to produce the right balance between the interests of all three parties, which sometimes (but by no means always) clash.

The principles of data protection fall under four headings:

- notifications
- data quality
- legitimate processes
- restricted access

to which it is convenient to add two factors which practically support them

- personnel
- control.

These headings, elastically interpreted, are believed to cover the whole subject of data protection, but it is not claimed that there are well-defined boundaries between their domains.

It will be noticed that these headings, as developed below, do not cover several issues which are often treated with data protection, such as the protection of national sovereignty, tariffs on transborder data flows, protection of jobs. These (whether admirable or damnable) are here considered extraneous to data protection.

In section 6.3 the complete range of possible regulations is covered (unless some are inadvertently omitted); it is not supposed that all of these will actually be found in any one set of regulations, and therefore phases like "the data user must" should be interpreted as meaning "a possible regulation is that the data user must".

6.3.1 Notifications

6.3.1.0 Introduction

Notification covers the need for facts relating to the system being made known in various ways. The motivation behind this is that people are much less apprehensive of systems about which they know, and about which they can easily find out more. It is further considered desirable

to inform the public generally about the ways in which personal data is used. This is embodied in the first principle in one of the first specifications of data protection:

> "There must be no personal data record-keeping systems whose very existence is secret." (H1:p.xx)

Related to this is what is known as the easy-access philosophy (F2), which wishes to make it as easy as possible for data subjects to find out what they are entitled to know, and correspondingly places the duty of disclosure and publication on others, in particular on the data user and the Authority. Badly-formulated requests for information (e.g. incoherent telephone complaints) should be handled sympathetically, and the data user should consider explaining the data subject's rights to him.

The various forms of notification are discussed below under three headings. Technical aspects of the data subject's right of access are also discussed in section 5.

6.3.1.1 Particulars of the systems

This refers to the requirements to disclose some particulars of the system variously to the Authority, to data subjects, and to the public:

1. The purposes of disclosure to the Authority are to enable the Authority to exercise control over the system, to give the Authority information to publish, and perhaps to provide the Authority with information about systems in general.

2. The purposes of disclosure to data subjects are to give them the opportunity to exercise their rights with respect to the system (e.g. to see a copy of the data which refers to them), to help them to know the likely consequences of their being data subjects and to reassure them that the system can bear scrutiny.

3. The purpose of disclosure to the public are to inform data subjects and potential data subjects of systems which may refer to them, and to raise the level of public awareness generally.

The following particulars of the system may have to be disclosed:

- its name
- its nature
- all uses and purposes
- the classes of data subjects
- the approximate numbers of data subjects in those classes
- the types of personal data held
- the sources of data

- all types of use within the organisation and the relationships of the users
- who outside the organisation has access to the data and for what purposes
- the person legally responsible for the system
- the person within the organisation and address who should be contacted for further information about the system
- where data is stored
- the retention period and method of disposal of the data
- the procedures to be followed by a person who wishes to know whether he is a data subject of the system, and if so to see the content of his record and to object to it.

The data user may also have to disclose promptly any substantial changes in the particulars given in the formidable list.

Under some laws, at least part of this information is published in a register, which provides the main means by which a person can find out of which systems he may be a data subject.

The extent to which, and the circumstances in which, this information must be communicated to the data subject will be stated in the regulations.

An additional requirement of the regulations may be to notify the data subject, when he is asked to give data, whether he is required to give data under some legal obligation and if so which, or whether it is a contractual necessity, or whether there is some other reason. He may have a right to know the consequences of a refusal to give the data.

A particular case of notification which is not often required is as follows:

> "Assure that no data about an individual are made available from the system in response to a demand for data made by means of compulsory legal process, unless the individual to whom the data pertain has been notified of the demand" (H1:p.63)

6.3.1.2 Data subject's access to his record

The regulations may provide that the data subject has the right to know what data referring to him is kept. This right may be subject to some restrictions for the benefit of the data subject, the data user or a third party. The circumstances in which the data subject can have a copy of his record may be specified, whether at a particular time (such as on entry to the system), or regularly (e.g.annually), or on demand by the data subject.

In any case, the form of the disclosure will probably have to be suitable for the layman, that is, be in plain language with all codes adequately explained. It may be that the real meaning of a data item is defined by the use to which it is put within the system, and to explain this to a data subject could be difficult.

The data user may be entitled to charge a fee in some circumstances for the disclosure to a data subject of his record.

The possible rights of a data subject to criticise the content of his record, and to make additions to it, are treated below under data quality (6.3.2).

6.3.1.3 Registration fee

It is convenient to include under 'notifications' the possible requirement of the data user to pay a fee to the Authority. This fee may be paid once, at the time of initial registration or licensing of the system (as in Sweden), or annually.

6.3.2 Data quality

This heading covers the requirements that the personal data should be true, accurate, sufficient, not misleading, up-to-date. It is convenient to include with

these the requirement that the data be no more than is necessary, and that it be deleted when it is no longer needed, though logically these follow from the principle of restricted access (6.3.4).

The implications of each of these requirements depend on the use which may be made of the data. For example, data is not up-to-date if it leads to decisions and operations which are substantially worse (particularly from the point of view of the data subject) than more up-to-date data would lead to. Again, the necessity of data is relative to how it is intended to use it.

Some data protection laws explicitly forbid the storage of certain types of data. For example. the Swedish law (S1: section 4), shows that permission will not normally be given for storing data relating to a person's criminal offences or health (among other things), and the French law (F1: article 31) forbids in general data indicating racial origins, or political, philosophical or religious opinions, or trade union membership. Such data would fail the test of necessity.

The Swedish law (S1: article 9) uniquely has a requirement that in some cases data relating to some persons must be included. This provision, which is covered by the above principle of sufficiency, is appropriate for such systems as those dealing with licenced drivers, improper exclusion from which could be damaging to the data subject.

Three further requirements which occur in the literature come under the heading of data quality:

1. The data subject's right to challenge the quality of data and add a note of dispute:

   "Maintain procedures that (i) allow an individual who is the subject of data in the system to contest their accuracy, completeness, pertinence, and the necessity for retaining them; (ii) permit data to be corrected or amended when the individual to whom they pertain so requests; and (iii) assure, when there is disagreement with the individual about whether a correction or amendment should be made, that the individual's claim is noted and included in any subsequent disclosure or dissemination of the disputed data." (H1:p.63)

2. What is termed error correction propagation (5.5) requires the previous recipients of data should be informed whenever the data needs correction or deletion (G1:pp.81-82).

3. The technique of depersonalisation permits the separation at an early stage of the part of the data which links it to a particular identifiable person from the part which is needed for the purposes of the system.

If this separation can be made completely and irreversibly the principle of necessity would require it to be done as soon as possible; if the possibility or re-linking the two parts of the data must be preserved, the princple of restricted access (6.3.4) requires that this re-linking be carefully controlled.

6.3.3 Legitimate processes

This section is concerned with the principle that processes which are carried out on personal data should be legitimate in the sense discussed below; the following section (6.3.4) is concerned with preventing access to data for other processes. 'Legitimate processing' covers three requirements:

1. The essential purpose of the system must be acceptable, for at least one of the following reasons:
   - it is agreed by all interested parties, in particular the data subject
   - it is authorised by the Authority, e.g. at time of licensing
   - it is explicitly required or permitted by law
   - it is disclosed by the data user in an adequate manner
   - it can be reconciled with social and moral considerations.

Under different systems of regulations some of these reasons may not be sufficient; for example the Swedish law (S1: section 2) admits only reasons like the second and third.

2. The individual processes within the system must be acceptable on similar grounds. For example, the collection of data by threat, deceit or invasion of privacy may be forbidden. The algorithms by which the system operates must be fair, e.g. not including unjustified racial discrimination or crude rules. Any data which is disputed by the data subject must be treated with appropriate reservations.

3. The processes must be carried out correctly, e.g. not impaired by program bugs or operator error in loading a wrong magnetic tape.

These requirements go to the very heart of the processing or personal data and have far-reaching implications for the data user. The first requirement is found in many formulations, e.g.

"Information should be regarded as held for a specific purpose and not be used, without appropriate authorisation, for other purposes." (Y1:p.183)

"There must be a way for an individual to prevent information about him that was obtained for one purpose from being used or made available for other purposes without his consent" (H1:p.xx)

data or processing which might lead to unfair discrimination needs special authorisation (E2:3)

"Personal data should be handled only to the extent and for the purposes made known when they are obtained, or subsequently authorised" (L1: section 21.09(2))

The second and third requirements are most referred to only obliquely in the literature, e.g.

"must take precautions to prevent misuse of the data" (H1:p.xxl)

"must not threaten human identity, nor human rights, nor privacy, nor the liberties of the individual, nor public liberties" (F1: article 1)

computer processing is not adequate for appraising human conduct (F1: article 2)

"Every person has the right to know of and challenge information and reasoning used in computerized processing" (F1: article 3)

"Precautions should be taken against any abuse or misuse of information." (E1:8)

"Care should be taken in coding value judgements." (Y1:p.184).

However, the Swedish Data Inspection Board feels empowered to intervene under section 6 and 18 of the Swedish law to prevent what are considered to be unfair processes (X1), and there is a trend of public discussion in this direction. For these reasons inspection must be at least capable of application to requirements for legitimate processing, whenever they find their way into the regulations.

However, in view of their quasi-judicial character, the inspector should beware of making decisions in terms of these requirements, but should report facts which he believes may be relevant to such decisions.

A further caution should be given against interpreting these requirements only in a negative form: often the interests of the data subject require not that the processing should be prevented because of some possible fault, but that it be carried out thoroughly and on time - a payroll calculation, for example.

6.3.4 Restricted access

This heading covers requirements that there should be no access to personal data except for purposes which are permissible as discussed in the previous section (6.3.3). There are several types of access to be considered, in computer parlance: read, write, amend, append, execute, erase. Of these, read access is the one of greatest concern in data protection, but the other types should be borne in mind.

Examples of this type of requirement in the literature are numerous, for example:

> "Access to information should be confined to those authorised to have it for the purpose for which it was supplied." (Y1:p.183)

> The Data Inspection Board shall regulate what data may be accessible, what may be issued, the keeping and selection of data, and its control and security (S1: section 6.6-9)

> the organisation must protect data "from any anticipated threats or hazards to the security of the system" (H1:p.55)

"Statistical data should be released only in aggregate form and in such a way that it is impossible to link the information to a particular person." (E1:10)

"Access to the information stored should be confined to persons who have a valid reason to know it." (E1:9)

The following requirements come under the heading restricted access:

1. The system should obtain data only from permissible sources.

2. Data within the system should be protected against access from outside the system.

3. Data should be accessed with the system only as permitted; if it is practicable to partition the data so that parts of the system which do not need some of the data cannot access it, that should be done.

4. Data should leave the system only to permitted recipients.

5. Data leaving the system should be depersonalised if possible (cf.6.3.2).

6. Statistical output should not permit fortuitous indentification of individuals (cf.L1: sections 26.06-9).

Several of these requirements are partly met by the security arrangements which are normal in good computer practice (cf.W1), but the emphasis for data protection is more on preventing information going out rather than preventing unwanted influences coming in.

6.3.5 Personnel

The requirements in the previous sections 6.3.1-4 are so numerous and far-reaching that they imply actions which in some cases will affect the whole of the organisation. Since this will involve many different sorts of people in the organisation, it is considered worthwhile to identify them here as a distinct aspect which must be inspected, although in a sense it is implicit in the previous requirements.

Some people would go so far as to say that the inspector should focus his attention primarily on the people in the organisation: if these are right, the system will be right; and if the people are not right, it is unlikely that the system will be. This is perhaps going too far:

1. Even good people have bad patches, and bad people have good patches, so their actual level of performance in important patches needs checking.

2. Some system are less dependent than others on perfect human operation, as discussed in the following section (6.3.6).

3. It is perhaps even more difficult to make a sound judgement of people than of mechanisms.

4. If the result from inspection are to be used in legal proceedings against the data user, objective evidence of a breach of the regulations is likely to be necessary.

In formulations in the literature this aspect is only occasionally made explicit:

> In the Swedish law, there is a responsible keeper of each file who has many duties, and must not reveal what he had learned about the personal circumstances of any individual (S1:13)
>
> An organisation should "Identify one person immediately reponsible for the system ..." (H1:p.54)
>
> It should "Take affirmative action to inform each of its employees ... about all the safeguard requirements ... (H1:p.54)
>
> Computer staff should be bound by rules of conduct and professional secrecy (E1:9)

The following requirements are intended to cover this aspect of data protection:

1. There should be a person who is identified as responsible for data protection throughout the organisation, with the authority, information and resources to see that all requirements are met.

2. All staff are selected, trained, given instruction, and encouraged to carry out their work with appropriate regard to the principles of data protection.

3. The working conditions facilitate the satisfying of data protection requirements.

Practical means for meeting these requirements will be treated in the inspection visit section of this report (6.5.2). At the present relatively early stage in the discipline of data protection, it is likely that many organisations will be uncertain about this administrative aspect.

6.3.6 Control

If an activity is important, it is worth devoting an appreciable part of the available effort to ensuring that the activity takes place as required. It is not enough to issue issue orders: one must check that they are carried out.

This is what is referred to here as 'control'. Experience of financial auditors indicates that control is an essential part of any complicated human system if it is to work satisfactorily. Some would suggest that the main task of an inspector is to check that appropriate control mechanisms (in the broad sense of the word) exists, and that they work as intended. Certainly this simplifies the inspector's work, and reduces the amount of direct checking of the system which is needed.

The method of working of control is this. Separate from the mechanism which is intended to perform some task, there must be a second mechanism which measures the quality and quantity of the first one's performance of its task, and has the means of correcting it when it is deficient. (An example of this sort of process is found in many branches of manufacturing, in which there is a separate department for quality assurance. Typically this takes samples from the end of the production line and tests them. If the standard of the samples is acceptable, the untested units are released for distribution. If the standard of the sample is too low, the whole batch from which they were taken will be rejected. And if too many batches have to be rejected, corrective action on the production line will be taken.)

The two stages (measurement or detection, and correction) are conceptually separate but are often combined. Inspection itself corresponds to the first stage, and a data protection inspector will therefore be impressed if the system contains its own internal inspection activity.

A related feature is what is called the resilience of the system, that is, its ability to perform acceptably as a whole when parts of it are performing badly. A common method of giving resilience to a human system is segregation of duties, so that the person who can authorise a step is not the person who can carry it out: such a step cannot be carried out when it should not be, unless both persons go wrong.

The control aspect of data protection is mentioned explicitly in only a small proportion of the literature:

> An organisation must be able to demonstrate that its system complies with the regulations (G1:p.96)
>
> "Data subjects should be able to verify compliance with these principles" (L1: section 21.09(5))
>
> The Data Inspection Board regulates control and security (S1: section 6.9)

6.4 The Inspection: preparation

6.4.0 Introduction

For convenience of treatment, the inspection is divided into three parts, roughly corresponding to before, during, and after the inspection visit.

6.4.1 Initiation of the inspection

It is the commissioning body which decides that a particular inspection must take place. For statutory inspections, this is the Authority, and the rest of this section relates particularly to such inspections.

There are several reasons which may trigger off an inspection:

1. As part of a procedure for licencing systems containing personal data, it may be necessary to inspect them before permitting them to operate. Except where prima facie the system is exceptionally dangerous from the point of view of data protection, this initial inspection would normally be so superficial as hardly to deserve the name, consisting merely of vetting of particulars of the system supplied by the data user.

2. Suspicion of a breach of data protection regulations, e.g. as evidenced by a complaint from a data subject.

3. Recognition that the time has come when a particular system should be checked for compliance: because it is potentially dangerous, or because a previous inspection (e.g. for licencing purposes) was not sufficient in some respect.

4. As a follow-up to check that faults revealed by a previous inspection have been corrected.

5. Spot checking of systems to encourage compliance with the law, to give general reassurance, or to provide information.

6.4.2 Factors conducive to inspection

In all cases except those in pursuit of a major complaint, the Authority will have some descretion over the urgency of a particular statutory inspection, and even whether it need take place. In assigning priorities to different inspections, the following should be considered:

1. The sensitivity and amount of personal data in the system.

2. The relationship of the data user and the data subject.

3. The motivation to abuse of the system.

4. The exposure to risk of the system.

5. Public apprehension about the system or the class of similar systems.

6. The likelihood of the system having changed since last inspected.

7. The convenience of the Authority.

The convenience of the data user may influence when but not whether a statutory inspection occurs.

Similar factors should influence the decision on voluntary inspection, but the convenience of the data user also may be considered.

It is likely that the total size of the statutory inspection activity will be decided by the Authority, and that this will then be divided under headings similar to those above. Since this is partly a political issue, the inspection policy and general programme of the Authority should be exposed for public discussion.

6.4.3 What is the system?

Sometimes it will be difficult to define what is to be inspected. This will not be the case for a spot check on a system whose particulars have been properly disclosed by the commissioning body. But if one suspects that there is a hidden system, or is pursuing a complaint, one may be uncertain which department of a large organisation should be inspected; in such a case the system for inspection purposes might have to be defined initially as the whole of that organisation's personal data handling, and the inspector would have the task of seeing if the inspection could be narrowed down to small parts of that system.

It is desirable that the system which is to be inspected should be specified precisely, as that will clarify the work of the inspector and the organisation; but absence of such a specification (e.g. because the commissioning body cannot get the necessary information) must not inhibit an inspection which is judged necessary.

6.4.4 Charging the inspector

The commissioning body, having decided that a particular inspection will take place, will appoint the inspector.

In choosing the inspector (who, it will be remembered from 6.1.8, need not be one person) the commissioning body will to consider several factors:

1. The expected amount of work in the inspection.

2. Technical aspects of the system which require special skills in the inspector, e.g. a particular computer operating system.

3. The importance of the inspection, e.g. public sensitivity, or significance for similar systems.

4. The abilities of available inspectors.

5. Plans for developing inspectors' abilities.

6. Other forthcoming inspections.

In appointing the inspector, the commissioning body should tell him any opinions it has on the desirable thoroughness of the inspection, its urgency and any other matters related to the inspection. The inspector should be equipped with any formal evidence he may need of the powers he has (6.2.3).

If the scope of the inspection is not the same as the full statutory requirements, its scope must be defined in the regulations (6.1.5).

6.4.5 Timing of an inspection

It will usually be more inconvenient and costly (at least in effort) for both the inspector and the data user if an inspection is carried out at short notice. Unless there is good reason for urgency (which will normally only be when there is suspicion of a serious breach which must be stopped quickly, or for which the evidence may disappear if the inspection is delayed), the inspection should take place at a time agreed by the data user.

The notice given to the data user will give him time to prepare for the inspection, which will usually reduce the time taken by the inspector. The time needed for this will vary; the Swedish Data Inspection Board (S2) allows about two weeks.

Notice to the data user does not mean notice to all staff connected with the system: it may be important for the inspector to see them in normal working conditions. There is a danger that the data user might use the notice time to improve the system and to fabricate or destroy evidence, thereby possibly deceiving the inspector. Three remarks seem in order:

1. If a forthcoming inspection has the effect of encouraging the data user to correct his system, the inspection will have served one of its purposes.

2. To the extent to which the past performance of the data user is important, any opportunity to impair the evidence relating to it is undesirable.

3. The inspection procedure must not be unduly influenced by hasty clean-ups by the data user are not likely to be maintained: for example, clear desks do not prove that printouts are never left lying about.

6.4.6 Approach to the organisation

Unless, for reasons discussed in the previous section (6.4.5), the data user is not to be warned that his system is to be inspected, the inspector will contact the data user before the visit. The following matters should be discussed:

1. The reason(s) for the inspection

2. The system which is to be inspected, including any information needed to specify it (6.4.3); what parts and aspects will and will not be inspected.

3. The expected scale of the inspection, in particular the length of the inspection visit and the number and identity of people forming the inspection team.

4. The powers which the inspector will have. What facilities he will need: working accommodation, computing. Conditions and methods of working.

5. What information should be sent to the inspector before the inspection visit (6.5.1).

6. Which people in the organisation will be involved, for what purposes and to what extent; which parts of the organisation may be visited; whether there is an internal inspector for the system; what documentation must be available (6.5.14).

7. When the inspection visit should occur. The data user or his substitute must be present during the visit.

8. Whether or not the data user will be shown the inspection report in draft and final forms.

The sole purpose of this discussion is to expedite the inspection visit by enabling the data user to transfer information to the inspector in a manner convenient to both; this will reduce the length of the vist and therefore the cost of the inspection. If the inspector can obtain the willing co-operation of the data user, the work will be facilitated (6.8.3).

In the case of a statutory inspection, written notice of the inspection and particulars of the inspection visit should be given to the data user, and he should be given the opportunity to find out what his legal rights are. Fig. 6.4.6-1 is based on the form of notice used by the Swedish Data Inspection Board (S2).

DATA INSPECTORATE Date: File No.....
Supervisory Department
(Official's name, forename and grade)

To: (name and address of the undertaking to be inspected)

ADP INSPECTION AT (subject's name and address)

We hereby confirm the agreement reached in our telephone conversation of today with (name and title) that the Data Inspectorate will exercise its powers of supervision by means of an inspection in accordance with paras. 15—17 of the Data Law (289 of 1973) at (undertaking's name and the address at which the inspection is to be carried out) on (date, time and duration).

The Data Inspectorate will be represented by:

(inspecting official's names)

The inspection will cover:

> (state here the particular purpose(s) that will later be put into the report under the heading 'Purpose of the Inspection' **or** a summary of the relevant items in the model report. How detailed the description is to be will depend on the circumstances of the individual case).

For and on behalf of the Data Inspectorate.

signed (the official)

fig. 6.4.6-1

6.5 The inspection: information gathering

6.5.0 Introduction

The central part of the inspection consists of collecting information to show the extent to which the regulations are being complied with. This information will consist of documents obtained from the data user and the organisation, answers to questions put by the inspector in the interviews with the staff of the organisation, and observations by the inspector of parts of the system.

In the following sections 6.5.1 to .14 questions to which the inspector must find answers are distributed under various headings, mostly corresponding to stages in which the system treats the data. This will not usually be the order in which it is most convenient to gather the information, which will depend on several circumstances, especially the way in which the system is organised. The inspector must use his judgement as to which of the listed questions need answering, bearing in mind the nature of the system, the regulations and the desired throughness of the inspection (6.2.6).

6.5.1 Preliminary information

It will be more convenient for both the inspector and the data user if as much as possible of the necessary information is obtained outside of the inspection visit. The informaion which is particularly suitable to obtain beforehand is this:

1. Legal documentation, e.g. data protection licence, previous inspection documentation.

2. The organisation; the general nature of its business, its size, management structure, any data protection policies.

3. Particulars of the system as in the staturoty declaration (6.3.1.1).

4. The system within the organisation; its importance, its management structure.

5. The parts of the system; where they are, what they are, how they fit together, who is responsible for each part, who can give information about each part; outline system documentation.

When he has analysed this information, the inspector should make an initial decision on the thoroughness of the inspection, and the parts of the system which he must inspect more throughly, so that he will be in a better position to plan the details of the inspection visit.

6.5.2 Personnel

As discussed in 6.3.5, the people involved in the system (including in principle the management of the organisation up to the highest level) are the most important single part of the system from the point of view of data protection, and therefore the inspector must form an opinion on them. The following questions should be considered:

- is there evidence that the highest level of management is aware of the legal and social significance of data protection, and of the need to organise to achieve it?

- does the organisation have a declared policy on data protection?

- is there a single person responsible for data protection throughout the organisation? does he have adequate resources? is he isolated from pressures to compromise data protection objectives?

- within the system, are there clearly defined responsibilities for all matters which relate to data protection?

- in the selection of personnel to work within the system, is weight given to the qualities which contribute to data protection, e.g. ability to respect confidences?

- are personnel within the system made aware of data protection responsibilities:
  - by initial training?
  - by notices?
  - by informal encouragement?
  - by periodic training?

- do working conditions generally support data protection objectives (this will be borne in mind throughout the following sections)?

6.5.3 Notifications

This section is concerned with checking that the data user complies with the regulations with respect to giving information of various types (and in one case, money) to various people.

1. To the Authority

- Is a declaration of the system sent to the Authority?
- Has the Authority received this declaration?
- Are all the required particulars present?
- Do the particulars correspond to the actual present system?
- Has the registration fee been paid to the Authority?

2. To the public

- Is the system disclosed publicly and by what media?
- Is the spread of disclosure adequate?
- Are all the required particulars disclosed?
- Are any particulars disclosed which should not be?
- Do the particulars correspond to the actual present system?
- Are the particulars as disclosed intelligible to those to whom they are directed?
- How are general queries about the system dealt with?
- Can the public easily find out whether or not they are data subjects of the system?

3. To the data subject

- Is the system disclosed to all the data subjects?
    - By what means?
    - Before entry to the system?
    - On entry to the system?
    - When data is collected from the data subject?
    - Regularly?
    - On demand by the data subject?
- Do the methods of disclosure work well (the inspector should consider whether to stimulate or simulate demands by data subjects)?
- How are demands (by letter, by phone, in person) dealt with?
- Do subjects know? ask a sample

- Are all the required particulars disclosed?
- Do the particulars correspond to the actual present system?
- Are the particulars as disclosed intelligible to the data subjects?

A similar set of questions applies to disclosure to the data subject of the content of his record, with these additions:

- What checks are made against impersonation of a data subject?
- What checks are made against a record being sent to a wrong address?
- Are any charges made for this disclosure legitimate?
- Is the data user informed of his rights to challenge the correctness of his record?
- How does a data user respond to such challenges by the data subject?
- Are corrections accepted?
- Are disagreements resolved satisfactorily?
- Is the data subject given a copy of his record after correction?

With regard to informing the data subject when data refering to him is passed out of the system for legal purposes:

- Is there a record of such occurrences?
- Is the data subject correctly informed?

6.5.4 Data capture

This heading covers all activities relating to the entry of data into the system. It is concerned to ensure that the process of gathering data is fair, reliable, confidential, and that any opportunities that it offers for informing the data subject are used.

The following questions should be answered:

- What sources of data are used?
- Can their accuracy be relied upon?
- Are duplicate or alternative sources available?
- Is unecessary duplication of data collection avoided (e.g. could data from different parts of the system or from other systems be used)?
- Is any source of data subject to other regulations, e.g. because it comes from abroad?
- Are the people who collect the data careful about accuracy?
- Are the people who collect the data careful about confidentiality?

- Are the input data forms:
  - Easy to understand?
  - Easy to fill in correctly?
  - Serially numbered for control purposes?
  - Suitably marked to indicate confidentiality?
  - Limited to the permitted data?
- Do any documents or human contacts with the data subject:
  - Declare to him the particulars of the system (6.3.1.1)?
  - Tell him whether he is legally obliged to give information, or the consequences of his not giving it?
  - Ask, or imply, his consent for the data to be used in some way
- Is improper pressure applied to the data subject (or any data supplier) to give data?
- Is the correction procedure error-prone or insecure in some way?
- Does the data subject receive a copy of the input data form?

6.5.5 Data entry

This heading covers all activities involving personal data after it has first been captured (e.g. on application forms) until it has been made fully available for use (e.g. has been key punched onto a computer disc). During this stage, the main dangers are that errors may creep into the data, and that confidentiality may be breached. The inspector should consider the following questions:

- Is the data during transmission into the system safe:
  - Against loss (e.g. are the documents serially numbered, and their movements logged)?
  - Against disclosure?
  - Against corruption, e.g. by mis-keying?
- Are punching documents stored securely when not in use?
- Are data preparation staff aware of the need for confidentiality?
- Can outsiders easily get access to the input documents?
- What checks on the accuracy of the data entry are made?
- What happens to the input documents after data entry?

6.5.6 Checking the data quality

This section is concerned with checking that the types of data in the system are permissible, and that their values are correct. The inspector checks all data storage media, and should answer the following questions with regard to the totality of data on these media. If a system has distinct parts such that it is inappropriate to lump all the data together in this way (e.g. because the flow of data between the parts has data protection implications which require control), the inspector has to treat each part of the system to some extent separately.

- What types of data are actually stored?
- Do these types correspond to what is declared?
- Do these types correspond to what is authorised?
- Why is each type of data needed by the system?
- How is each type of data used in the purposes of the system?
- Would extra types of data improve the quality from the data subject's viewpoint?
- How are requests for inclusion of each new type of data authorised?
- What steps are taken to ensure that the data is:
    - Accurate
    - Up to date
    - Not misleading
    - Complete
- Is the data actually:
    - Accurate
    - Up to data
    - Not misleading
    - Complete

- How many external (e.g. from a data subject) corrections are received?
- Are they effectively processed, included in backup copies?
- How are disagreements over the values to be recorded resolved?
- Are there any procedures for propagating corrections to those who have received incorrect data?
- What procedures are there for deleting data when it is no longer needed?
- Do they work?

6.5.7 Restricted access

The requirements of restricted access apply to data in all the forms which it may take within the system, including human-readable hard copy, computer storage of all types, data in transmission (e.g. by cable), and even the human mind. These are so pervasive that it is simpler for the inspector to check accesses to all parts of the system, rather than just to the data which is the prime concern of the regulations. Indeed, the West German Federal Data Protection Act (D1: annex to section 6(1)) explicitly requires controls of admission, leakage, memory, user, data access, communication, input, processing on behalf of third parties, and transport (as well as organisation control, which is covered here in 6.5.2)

The inspector is therefore challenged to check that there is no access to any part of the system (accommodation, hardware, program, data storage media, papers, human beings) except that which is permitted, and that the nature of each access is as permitted (e.g. that a person permitted to access a file for one data subject's record does not browse through the file out of curiosity). In considering the following questions, the inspector may therefore wish to concentrate on the main issue, viz. can anyone read data which he should not?

- Is physical access to the accomodation in which the system is located confined to those who need it?
- Within the system, is access to each part confined to those who need it?
- In what media is data stored?
- What procedures exist for determining who should have access to the data in each of its forms?
- Do these procedures correspond to the accesses required by the declared purposes of the system?
- Are they effectively administered?
- What precautions are there against improper access by authorised persons (e.g. browsing)?
- Are there any undisclosed data files?

The above questions apply to many parts of the system. The following are examples of questions related to specific parts in the computer area (for a more nearly exhaustive set of check points, see ref. W1):

- Are computer terminals housed in secure locations?
- Is access to computer terminals confined to authorised personnel?
- Is there a computer log recording all input files accessed and the pesons and programs which accessed them?
- Does the computer log record all output files which are produced?
- Is oversight of sensitive information prevented, e.g. by placing a VDU so that the person using it has a blank wall behind him?
- Is there a media librarian who enforces physical controls on the media library?
- Is there an effecive computer password system which confines use of computing facilities to authorised personnel?
- Does the computer operating system provide effective lock-outs of data, both in the main store and in backing store?
- During program development, is care taken that tests are not run on sensitive data?
- For transmission between remote stations, and storage, is encryption used?
- Are print-outs containing sensitive data removed promptly and kept from places where they can be read by unauthorised personnel?
- Is photocopying of such printouts prevented?
- Where possible, is data partitioned, so that users cannot access parts of the file which they do not need?

6.5.8 Data update

This heading covers the requirement of ensuring that the personal data which is held within the system is kept up-to-date, including any correction and rearrangement of the data. As explained in 6.3.2, the required degree of up-to-dateness is that which will avoid the data processes producing wrong results, and will therefore be different for different data items. In many cases there will be some element of judgement involved. With this in mind, the inspector should ask the following questions:

- How up-to-date should each data item be?
- Does the data user have an idea of the up-to-dateness required? how does it compare with the inspector's opinion?
- What measures are prescribed to keep the data up-to-date?
- Are these measures carried out?
- Is the data in fact up-to-date?
- Is the updating applied to any back-up copies of the data which are kept?

6.5.9 Data use

This heading covers all processes, including human operations, by which the data is manipulated to satisfy the purposes of the system. It would include such actions as payroll calculation, a search through police intelligence files, the maintenance of a hospital administration system. The main interests of the inspector under this heading are that only duly authorised processes occur, that they are correctly carried out, and that the processing does not expose the data to improper access. He should ask these questions:

- What are the declared purposes of the system?
- What are the actual uses of the system?
- What is the procedure for authorising processing of data?
- Is it appropriate, considering the nature of the data?
- Is it correctly observed?
- What processes are carried out?
- Are they suitably authorised?
- Are they necessary and legitimate?
- What checks are there that no other processes are carried out?
- Do the processes treat ambiguous or unreliable data appropriately?
- Is the logic of the programming fair, especially to the data subject?
- How is the programming done?

- Is it adequately checked?
- Is the programming correct?
- Are the systems programs checked?
- Do the programs include checks against:
    - data error
    - programming error
    - operator error
    - machine error?
- How are the programs protected against accidental corruption?
- How are the progams protected against deliberate corruption?
- How are amendments to the programs:
    - initiated
    - checked
    - authorised
    - implemented?
- Are the (computer) operations correctly executed?
- Are any interests of the data subjects with respect to the reliability of the processing (e.g. in the event of partial failure of the system) protected?

6.5.10 Data interrelation

This heading refers to the possibility of data from different systems being brought together to give what is felt to be a qualitatively different collection of data. Although this is logically covered by the headings of data capture (6.5.4) as regards data coming into the system which is being inspected, and data dissemination (6.5.11) as regards data going out of the system, the public concern which is associated with such activities requires the inspector to take special care to examine them. The following questions should be considered:

- From what other systems does data enter the inspected system?
- What data enters from these systems?
- To what other systems does data pass from the inspected system?
- What data passes to these systems?
- Are these transfers:
    - authorised suitably?
    - declared suitably?

6.5.11 Data dissemination

This heading covers all personal data which leaves the system deliberately (i.e. by the decision of the data user), whether in machine-readable or human-readable

form; but notifications to the data subjects are covered in 6.5.3. The requirement is that such data should not cause improper disclosure. The inspector should find answers to these questions:

- What data leaves the system?
- Is this dissemination a part of the declared purpose of the system?
- If not, is it suitably authorised or otherwise permissible?
- Is its reciept declared by the recipient?
- Is the method of transmission secure against corruption and unauthorised access?
- In particular, are human-readable documents suitably protected against unauthorised reading?
- Are checks made that persons cannot be inadvertently identified, e.g. in statistical tables (6.3.4)?

6.5.12 Data archival

In many systems there are arrangements for segregating data so that it is not ordinarily avilable for processing, but can for special purposes be accessed by special means. This segregation of data is what is here referred to as archival. Data is usually archived when it is no longer expected to be frequently used, but should not be erased because it might be needed. This

archiving is desirable in the name of data protection, as it prevents the data being readily accessed, so the inspector should see that archiving is used whenever possible, and that the data is adequately protected:

- What arrangements are there for archiving data?
- Are they used as much as they should be?
- Do they work properly?
- Is archived data kept securely?
- What are the arrangements for retrieving archived data?
- Is archived data kept securely against unauthorised access?
- What interest has the data subject in archived data?
- Is archived data erased when it is no longer needed?

6.5.13 Data erasure

The term 'erasure' is used here in its normal sense as referring to the process which puts data so that it is impossible ever to read it. This is the last thing that can happen to data, and it is sometimes considered the ultimate in data protection. But the interests of the data subject and society at large will often require that data should be retained longer than the interests of the data user would require; e.g. as a legal requirement, or

for the purposes of scientific or historical research. The inspector must therefore check that data erasure takes place at the right time, and is carried out effectively:

- Who decides when each item of data is to be erased?
- Are these decisions suitable, bearing in mind particularly the subjects' interests?
- What are the procedures for erasing data in all its forms:
  - human-readable paper?
  - punch cards?
  - paper tape?
  - magnetic tape?
  - magnetic disk?
- How are they carried out?
- Are they duly carried out?
- Are they effective, e.g. no residual images on magnetic tape or disc?
- Are documents and carbon papers shredded?
- Are there any plans for disposal of the data in the event of termination of the whole system?
- Are there any threats to the subject in improper (accidental, malicious) erasure?

6.5.14 Control

As discussed in 6.3.6, control is a vital aspect of the organisation's data protection work. As such, it applies to all the other items which are inspected, and should be borne in mind by the inspector throughout his gathering of information. The following factors should be considered:

1. Documentation. This should describe the system so that there is no doubt what should happen in each part of the system at each stage of the processing of the data. It should be correct, which requires that there must be a means for keeping it up-to-date.

2. Logging. There are many events occuring within the system, and a perfect log would make it possible to find out what has happened in the past, and what the current situation is on any particular, so that in principle one could have a complete action reply. The inspector should check that complete and accurate logs are kept of all significant routine events, e.g. receipt of batches of personal data, computer runs, mail outs, and of all significant occasional events, e.g. enquiries from data subjects, computer breakdowns, personnel changes. It is technically feasible for a computer to log all the accesses which are made to files of data, and this is considered a powerful aid to data protection (G1:pp.49-53, 144-5).

3. Error detection and correction. An error is any occurrence in the system which is not intended by those who specify it; the word is used here to include deliberate interventions (e.g. for private gain) as well as accidents. It is inevitable that errors will occur, and therefore there must be means to correct them. The particular means will depend on the process in question. for example, key-punching from input documents may be checked by being repeated by the same (or preferably a different) operator. Streams of numbers can sometimes be checked by seeing if their total is correct. Discrete electronic transmissions will usually have checkbits which in some cases permit automatic correction of errors. The inspector should find out whether at all important stages where errors may occur there exist suitable means for detecting and correcting them.

4. Separation of duties. A potent device for reducing the risks arising from human fallibility is the practice of arranging that at least two persons are needed before certain actions can be taken. In some cases the roles of the two persons are equivalent (e.g. holding two keys to unlock a store of sensitive data); in others one person is needed to authorise the action before the other takes it.

5. Internal inspection. The inspection procedure which is described in this section 6 is intended to be adaptable for use by an organisation on its own

systems (6.2.4). Some organisations could justify maintaining their own inspection departments continuously monitoring data protection in all parts of the organisation. If such an activity exists, it is likely that the level of compliance for the regulations will be high, or if not high at least it will be known, and that the work of the external inspector will be lightened; but it does not excuse the external inspector from carring out his own checks independently.

The following questions summarise the issues which the inspector should keep in mind under the heading of control:

- What documentation of the system exists?
- Is it complete?
- Is it clear?
- Does it agree with the system that exists?
- What mechanism is there for keeping it up-to-date?
- What logs are kept of routine events?
- What logs are kept of occasional events?
- Do they give adequate records of what has happened?
- Do they make it possible to determine what the current situation is?
- What means of detecting errors are there?
- How are detected errors dealt with?
- At important points in the system, is the principle of separation of duties applied?
- Is there an effective internal inspection activity?

6.6 The inspection: conclusion

6.6.0 Introduction

When the inspector has gathered all the information which he needs, his remaining duty is to produce the inspection report. The means of presenting this is discussed in 6.6.1, and its contents in 6.6.2. When it has received the inspection report, the commissioning body must decide if any further action is required (6.6.3). The inspector may report to the commissioning body further information which is not in the inspection report (6.6.4). At the end of the inspection, the materials which have been fathered by the inspector must be disposed of satisfactorily (6.6.5).

6.6.1 Presentation of the inspection report

The formalities of the inspection report are these: since the inspector is appointed by the commissioning body, it is to that body which he presents his report, and it then belongs entirely to that body. The report is concerned only with meeting the purposes of the inspection. But this will never be the whole story:

1. The inspector would be wise to discuss his report in draft form with the commissioning body, to check that it meets the objectives of that body and if necessary to make improvements.

2. The inspector should send a copy of his report in draft form to the data user (unless, as discussed in 6.8.5, there are compelling reasons against this action), and, if appropriate, react to his comments.

3. The commissioning body will usually send a copy of the final report to the data user (6.6.3).

4. There will be much useful information which the inspector should consider passing on to the commissioning body less formally (6.6.4).

6.6.2 Inspection report - contents

The formal result of an inspection is a report which the inspector send to the commissioning body. To meet the essential objectives of inspection (6.0.2), it must

contain sufficient detail of all discovered actual or potential breaches (6.2.1) of the regulations, so that the commissioning body can decide what should be done; or, if there are nod discovered breaches, it must say so.

The following should be in the inspection report:

1. Identity of the system which is inspected: its name, address, the organisation, the data user, any legal registration particulars; the time (point or period) to which the inspection applies.

2. Purpose of the inspection, its scope and a description of the regulations on which the inspection is based.

3. Name of the inspector.

4. Particulars of the inspection visit: time, places, people interviewed.

5. Any necessary general information about the system; if the purpose of the inspection is to provide information to the Authority (e.g. to enable it to oversee personal data applications generally), this may be a substantial section.

6. Particulars of any discovered actual or potential breaches, or if there are none, a statement to that effect. If the system has been registered as required

by the regulations, this will be stated here. This section which for statutory inspections is normally the essential core of the report, may actually be a small, or even almost empty, part.

7. Other remarks about the system which, though not formally necessary, could contribute to good personal data practice. Reference could be made to problems (and perhaps solutions) which might be relevant to other systems, and be of interest to computer manufacturers, etc. It may be convenient to present this as a review of the whole system, perhaps structured in a similar way to the inspection visit (6.5), commenting on its strength as well as its weaknesses, and recommending methods of improvement. For voluntary inspections, this will normally be the most important part.

8. Particulars of any intended follow up action, e.g. a further inspection to check whether necessary improvements to the system have been made.

A translation of a model for the inspection report which is used by the Swedish Data Inspection Board (S2), is shown in the figure below.

DATA INSPECTION BOARD
Supervisory Department

REPORT

(date of inspection)

Inspection of ADP/Register of Persons at (the authority of firms address)

Inspection Officials. Names and forenames of the representatives of the Data Inspection Board.

Representing (the authority or firm). The authority or firm's representatives during the inspection: names and forenames and, if relevant, their positions.

Time. For example, 9—12 noon, but also the date if the inspection extends over more than one day.

Purpose of the inspection. The heading is to be used if required where the purpose of the inspection must be given in more detail than is shown in the headings given in the report.

Organization and its business. The authority, organization, company, management and owners.
Business: internal, external
Installation: development, operation.

Own register of persons

— Own register (or list)
— Check of authorization
— Secrecy declarations or other sensitive registers or information.

Work carried out for other organizations

— Customers' registers or persons (or lists)
— Obligations according to the agreement with the person(s) responsible for the register
— Powers of attorney
— Information to the customers regarding the Data Act.

Check of Authorization

— Compliance with conditions as in Sections 5, 6 and 18
— Routine amending as in Sections 8 and 9
— Routine reporting as in section 10
— Other relevant measures

Layout and premises

— Computers, terminals (number, type, performance and distribution)
— Data communication
— Condition of the premises.

Security of Data

— Security organization; instructions
— Secrecy pledge as per section 13
— Check of authority in batches/real time
— Handling procedures; system documentation
— Operating plan, shift rota, etc. control of access, visitors' book
— Reconstruction
— Data media: receipt, issue, preparation, follow-up tape library
— Weeding, cancellation of magnetic tape/transcription.

Data quality

— Data acquisition
— Coding
— Data recording
— Processing
— Outgoing data

Inspection of the Register

— Register transcription, outgoing data; check of authorization.

There is nothing further to be added to the report.

Signature of the Official

6.6.3 Subsequent actions by the commissioning body

The commissioning body will normally send a copy of the inspection report to the data user (6.8.5), with a covering letter.

The commissioning body must review the inspection report. If it decides that no action is required by the data user, it should tell him of this decision, and tell the inspector to dispose of his inspection materials (6.6.5). The commissioning body may decide that actions are needed with respect to the system:

1. It may order the data user to make changes to the system in specified ways (even to the extent of stopping its operations temporarily or indefinitely).

2. It may suggest to the data user that changes are made to the system.

3. It may give notice of its intention to re-inspect after a stated time interval.

4. In the case of a statutory inspection, it may initiate prosecution of the data user.

The next page is a translation of a model of a letter which may be sent by the Swedish Data Inspection Board to a computer bureau following an inspection which revealed deficiencies in the system.

DATA INSPECTION BOARD Date: File No.....
Supervisor Department
(Official's name, forename and grade)

To:
(The name and address of the subject of the inspection)

ADP INSPECTION OF (the name and address of the subject of the inspection)

Herewith a copy of the report on the inspection of your undertaking carried out on 28 February 1978.

Under the provisions of section 18 of the Data Act, the Data Inspection Board may, as a consequence of what emerges from the inspection of a computer centre, amend the conditions previously laid down in the Certificate of Authority to establish and operate a register of persons, or may issue new directions in the respects stated in section 5 or section 6 of the Data Act. By law, such directions must be addressed to the person(s) responsible for the register, for example, a service agency's clients/customers, who maintain a register of persons with the service agency.

Following the inspection carried out at your premises, the Data Inspection Board is considering issuing directions in the following respects:

> (Description of deficiencies noted; person(s) responsible for the register and the register for which the new directions are being considered).

As a step in the handling of this matter, the Data Inspection Board provides you with an opportunity to make any comments you may wish to make on the inspection report and the deficiencies mentioned in it by not later than...197....

Your comments should show whether, and if so by what date at the latest, you intend to take any steps to correct the deficiencies. Your comments must include a statement of what the proposed measures will consist of.

For and on behalf of the Data Inspection Board.

(Signature:

The statutory inspection should give sufficient information for the Authority to make a sound decision within its responsibilities (e.g. whether to prosecute the data user for breach of the regulations), but not with the other factors which would influence such a decision. It is important that an inspection which may be the basis of legal proceedings should produce evidence that is strong enough to withstand forensic handling.

6.6.4 The inspector's other findings

Apart from the esential hard facts which form the main contents of the inspection report, or are their basis, the inspector may gather a great deal of additional useful further information, including:

1. The inspector's impressions of the system, the data user and the organisation with respect to data protection.

2. Experiences during the inspection which may be relevant to future inspections, e.g. testing methods which work well or badly, unexpected problems and unusual solutions, undesirable pressures on the inspector (6.7.5).

3. Insights which should influence future policy towards inspection of the system or others like it.

Such information is cumulatively of great value, and should not be discarded because it may be controversial, subjective or difficult to present. For example, the Authority needs it to carry out an effective inspection programme. The inspector should therefore find means of passing this information to the commissioning body. The question of the breaching confidences of the data user is considered in 6.7.8.

The commissioning body must decide whether this information should be disclosed (e.g. to the data user).

6.6.5 Disposal of inspection materials

When the inspection is complete (i.e. when the commissioning body has decided that no further action will take place), the documents and any materials required by the inspector are no longer needed. The interests of the data user, and perhaps the data subjects, requires that these be correctly disposed of, by being returned or destroyed.

However, it may facilitate a subsequent inspection of the same system if some of the materials are retained. This should be done only with the consent of the data user, and what is retained should be agreed by the data user and the commissioning body. The commissioning body rather than the inspector should be responsible for retaining these materials, and must make suitable arrangements for their security.

If the Authority decides to retain some materials within its legal powers (e.g. for its own analytical or statistical purposes), information ethics requires that the data user (and perhaps the data subject) be told what information is stored, by whom, for what purposes, for what length of time, and who will have access to it.

6.7 The inspector

6.7.1 The inspector's qualities

The following qualities are required in the inspector:

1. Understanding of data protection. He must appreciate the public concern in this matter, and be familiar with the means which are proposed for preventing troubles arising from personal data. He must understand the regulations, and be able to interpret them in practical terms, and work out their implications for the system which is being inspected.

2. Experience in the way human beings in organisations work. He must recognise the significance of such factors as authority, bureaucracy, habit, laziness, corporate ethos.

3. Up-to-date knowledge of any technology used in the system, e.g. computers, communication links, encryption.

4. General inspection skills, such as can hardly be acquired except from experience in auditing, investigation or other inspection: e.g. interviewing, a nose for something wrong.

5. Trustworthiness. The inspector must have access to information on which the data user places the highest degrees of secrecy (e.g. confidences of clients, security arrangements, trade secrets). The inspector must have the integrity and ability to protect such information throughout the inspection and afterwards. In some cases (e.g. for national security systems) the information must not be disclosed even to the commissioning body.

6.7.2 Who should inspect?

Although all these qualities (6.7.1) are not necessary in the highest degree in every inspector, they represent an unusual array of gifts. Perhaps only a team consisting of several persons will contain them all. Computer expertise of a special type may have to be bought in on contract.

Even if gifted individuals are available, there are advantages in having at least two people carrying out an inspection: apart from compensating for each other's deficiencies, they can check each other's work, give second opinions on certain matters, serve as a sounding-board for

fresh ideas, and stand back when the other in involved (e.g. in an interview). In addition, they reduce the effectiveness of possible corrupting pressures (6.7.5), and give more confidence in the objectivity of their report.

The wide range of gifts required in an inspection forms the basis of a professional specialism, and it is to be expected that organisations specialising in data protection inspection will arise. It is in the interests of all concerned in the correct use of personal data that this profession is properly structured with regard to such matters as training, technological updating, qualifications, career development, professional ethics.

It is not necessary that the Authority should directly employ full time inspectors, but it must be able to call on then when necessary to carry out statutory inspections at its own instigation. The Authority must satisfy itself that any inspectors whom it uses are competent.

6.7.3 Relation to financial auditing

It is sometimes suggested that financial auditing is an existing profession which could with a little effort expand to include data protection inspection. Of the qualities listed in 6.7.1, financial auditors already need for their work items 2, 4, 5; some use item 3; none need item 1. It follows that financial auditors as such are not competent to carry out a data protection inspection.

But they may be the best-placed group to move into this area, if they acquire the qualities in which they are at present deficient. Two additional factor favour them:

1. Financial auditing is already accepted as routine by parts of most organizations, and auditors are received in a co-operative spirit.

2. Sometimes it may be possible to combine the data protection inspection with a financial audit, with advantages for both sides.

6.7.4 Questions of judgement

It will be clear from many parts of this report that the inspector must make judgements on a wide variety of matters. The purpose of this section is to point out that his work will take him into areas where his opinion is not authoritative. What these are will depend on the scope attributed to the inspector, but they will probably include interpretation of the regulations where they are not precise.

It is important that the inspector does not go outside the areas of his competence, and therefore that he should have some means of disposing of such matters. This will normally consist of passing them up to the commissioning body for a decision.

6.7.5 Pressures on the inspector

The data user may apply several types of improper pressure to the inspector:

1. Time: It may be said that too much time is being spent on the inspection, particularly if it is taking longer than was planned.

2. Cost: The data user may argue that his work is being excessively disrupted by the inspection activity.

3. Obstruction: The inspector may find that his work is made increasingly difficult by non-co-operation, delays, unnecessary complication, and even sabotage.

4. Sympathy: The suggestion may be made that although the system is faulty, the people concerned are doing their best and cannot usefully be penalised.

5. Politics: e.g. complaining or threatening to complain about the inspector's head.

6. Bribes: Not only money, but any measure to please the inspector personally to induce him to leniency.

7. Bluff: e.g. suggesting that if the inspector knew his job he would be satisfied with the information he had. Attempts may be made to overload him with excessive amounts of documentation.

8. Personal: e.g. overbearing VIPs.

No uniform means of neutralising these pressures can be relied upon. The inspector must be aware of their possibility, must know how to recognise them, and must have multi-faceted integrity to resist them. His task is

made easier to the extent to which he is supported by the commissioning body. He should include in his report comment on any substantial attempts to use improper pressure.

6.7.6 How helpful should the inspector be?

The principal purpose of the inspection is objective assessment of the system. To combine this with directly helping the data user to improve the system risks blurring responsibilities: measurement and correction are separate activities, and one should beware of compromising the former for the sake of the latter.

However, the ultimate aim of inspection is to improve performance in data protection, and at present there is not so much knowledge and experience that one should willingly silence one source of information. On the content, meaning and implications of the law, for example, the inspector will probably know much more than the data user.

The question of giving advice about the system is more controversial, but even here the balance of advantage to the community suggests that the inspector be permitted to advise the data user, provided that he is careful not to let this distort his judgement as inspector, nor prejudice further inspections by implying that if his advice is followed subsequent inspections will approve the system. He must be careful about exposing himself to financial pressures by selling consultancy to an organization which he inspects; this must impose tight limits on the scale of the advice he can give. As in any matter which might compromise the inspector's role, the commissioning body should be kept fully informed: the inspector should report the general content and scale of any substantial help he provides to the data user.

In a voluntary inspection, the duty of preserving the independence of the inspection may not be so great as to overrule the value of involving the inspector in improving the system.

6.7.7 Complaints against the inspector

It is unsafe to assume that the inspector will be perfect, per therefore provision must be made for checking his work and dealing with criticism, whether justified or not. In the case of a voluntary inspection, the commissioning body and the organisation are either identical or so close that the controversy is essentially an internal matter. In the case an of a statutory inspection, the law is involved, and it is therefore a matter of public concern to resolve disagreements satisfactorily.

The following may be expected to be the main source of controversy between the inspector and the data user (objection to the decision to inspect, perhaps on grounds of frequency of inspection, should be addressed to the commissioning body or the one which made the decision):

1. Objection to the extent of the inspection's interference with the work of the data user.

2. The right to withhold infomation which is considered inessential for the inspection, even if it would facilitate the inspector's work.

3. Lack of trust in the inspector personally.

4. Disagreement with the interpretation of the regulations.

5. Disagreement with the interpretation of the evidence.

It is conceiveable that a data subject or a member of the general public might have some criticism of an inspector or inspection. If any party objects to any aspect of the inspection, it should have a clear line of complaint to the commissioning body. In the case of statutory inspections, there must be a means of complaining against the commissioning body. This entails that the commissioning body should not be the final legal authority, or at least that, if they are both roles of the authority, these roles are seen to be independent.

The commissioning body should ensure that the data user knows his rights of complaints and his means of exercising them.

The philosophy of Section 6 is that any important activity must be checked. Inspection is such an activity, and it is therefore desirable that the commissioning body should take steps to ensure that inspections are carried out correctly from every point of view.

6.7.8 The inspector's answerability

Since the inspector is appointed by the commissioning body, he is primarily answerable to that. However, claims on his loyalty come from at least two other directions:

1. The law: A citizen is normally expected to report evidence of any criminal action which he knows. If as part of his inspection he incidentally discovers an illegality which has nothing to do with data protection, must he report it?

2. Ethics: Working relationships between two parties such as the inspector and the data user, are inefficient unless there is some degree of mutual respect. Does this require the inspector to connive at minor deviations from the regulations?

There can be no easy complete answer to such questions which overlap conflicting obligations. Until such time as the inspection activity has been established by experience, the inspector should be wary of giving so great a weight to any one obligation that it effectively overrules the others. This would suggest that the inspector should concentrate on the substantial matters which are important from the point of view of data protection.

The one exception to this suggestion of overlooking minor deviation is that of corruption: any attempt to bribe an inspector is potentially so dangerous to th whole inspection activity that it should be reported to the commissioning body. Consideration needs to be given also to means of helping an inspector to resist improper pressures from the commissioning body.

6.8 Further considerations

6.8.0 Introduction

In section 6.8 are discussed all issues relating to inspection which did not fit in anywhere else.

6.8.1 Frequency of inspection

The ideas behind repeated inspection of one system are twofold. Firstly, there may be some doubt about the effectiveness of the first (or indeed any single) inspection of the system. Secondly, it may be believed that the system has changed sufficiently since last being inspected, so that it is to a considerable extent an uninspected system.

As regards to the first, it must be recognised that no inspector and no inspection is perfect, and hat if the system presents a very serious risk (e.g. because of the data which it holds, or because of its method of working) and is difficult to inspect thoroughly (e.g. because of size or complexity), a repeated inspection, even within a short time, may be justified. The inspector should be encouraged to comment to the commissioning body on the suitable interval before the inspection, as his subjective assessment of the effectiveness of his inspection may contain information for which he cannot produce evidence.

As regard to the second, the data user may be required to notify the commissioning body whenever there is a substantial change to the system, such as might warrant re-inspection. If there is no such requirement, or if there is suspicion that the requirement it not complied with, more frequent re-inspection is justified. The commissioning body should in such cases judge the likelihood of such a change taking place, bearing in mind both the nature of the system (as being conducive to change or not), and the motivation of the data user; in this, again, the unproveable opinion of the previous inspector may be valuable.

Since both of these possible reasons for repeated inspection depend on the system and other particular circumstances, no single frequency (such as once a year) can be generally recommended.

6.8.2 Strictness of inspection

The inspection procedure described in sections 6.4 to 6.6 is intended to be capable of being almost exhaustive in

its scope and depth. For many inspections such as thoroughness and consequent costs may be considered inordinate, and the inspector should select parts of the procedure which he thinks will give him sufficient information.

For planning purposes, he may have to take an initial view of the desirable level of strictness; this may be based on unreliable information such as the reputation of the organization. At an early stage in the inspection he should attempt a more reliable judgement, still based inevitably on incomplete information, but good enough for operating purposes. Inspectors in other areas (financial auditing, taxation) claim that they can very quickly sense the general level of performance of the system which they are inspecting. As a first step, the inspector's impression of the awareness and ability of the management of the organization (6.5.2) will be a good guide.

The inspector must be prepared to change his level of strictness as the inspection proceeds, it the accumulated evidence justifies it. He should beware of being prejudiced by his first impression, and must be willing to apply very different levels of strictness to different parts of the system. He should have in mind three different patterns of compliance:

1. Fairly uniform throughout the system, whether at a high or low level of compliance.

2. A much lower level of compliance in one or more small parts, caused primarily by negligence, and with no great effort to concealment.

3. An intolerable failure in one or more small parts, due to an essential violation of the principles of data protection, and possibly with a serious attempt at concealment.

The prevailing opinion in data protection circles at present is that the first two of these patterns are by far the most common, and therefore most inspections should be conducted in a manner suitable for them. But much of the public concern is focused on the third pattern, and an inspection method which cannot expose such systems will generally be considered useless.

6.8.3 Attitude of data user

The attitude of the data user may make a great difference to the inspector's work. If he is co-operative, open, efficient and sympathetic the work will be much easier and more efficient. The inspector should therefore seek to encourage such attitudes.

However, the inspector must not depend on meeting such attitudes, and if he does meet them must not rely excessively upon them instead of doing the work himself. He must not simply accept everything he is told. If the data user never feels at least slightly uneasy, the inspector is not being effective (unless the system is extraordinarily near to perfection).

6.8.4 Secrecy of inspection procedure

It might be feared that disclosure of the procedure which is followed by inspectors would diminish its effectiveness. An unscrupulous data user might discover blind spots which he could exploit. This risk appears fairly small, and in any case the procedure must not be so rigid and static that it contains reliable loop-holes (cf. 6.2.5). If there is a large permanent flaw in the procedure, the sooner it is exposed and removed the better. A procedure which depends on long term secrecy is vulnerable.

There are however some tactical details whose secrecy deserves consideration: for example, the timing of unannounced inspections, which particular samples of data will be examined. These are not fixed items in the inspection procedure of the type which is discussed here.

Otherwise, there are advantages in disclosing details of the inspection procedure: it will help to de-mystify the subject in the minds of data users; it will reassure them and the public that the procedure is efficient and practical; it will help data users to comply with the regulations by encouraging self-inspection. These advantages decisively favour disclosure of the procedure.

6.8.5 Publication of the inspection report

The inspection report is the property of the commissioning body, and the main purpose of the inspection (checking the system's compliance with the regulations, 6.0.2) does not require the report to be disclosed to anybody else. The following are the arguments against further disclosure:

1. It could give the data user help in tampering with evidence which might be used in legal proceedings against him; for example, he might improve his security arrangement.

2. It might expose the inspector to a charge of defamation.

3. It might prejudice legal proceedings against the data user.

4. It might compromise the security of the system and others like it, and breach confidences of the organization.

5. It might give an insight into the inspection process which could help exploitation of its weaknesses to avoid detection of non-compliance.

6. The inspector may be inhibited from making clear criticisms, because he would have to spend excessive time preparing defences for his conclusions.

The following are the arguments in favour of disclosure of the inspection report to the data user:

7. It is normal professional practice (e.g. in financial auditing, computer security consultancy) to show a draft of the report to the inspected organisation. This tends to improve the quality of the report by removing errors and unbalanced judgements; it increases the confidence of the data user in the fairness of the inspection, and (if he know beforehand) will encourage his co-operation in the inspection; and it tends to forestall criticism of the report.

8. It helps the data user improve his system from the point of view of data protection.

The following are the arguments in favour of publishing the inspection report:

9. It tells the public, including therefore the data subjects, about one of the most important qualities of the system, viz. does it satisfy the regulations?

10. In conjunction with other inspection reports, it gives the public information about the general state of data protection, thereby justifying confidence or alarm.

11. It might give data users information about data protection measures, thereby tending to improve the general standards of performance.

Because of the advantages of disclosure, particularly at the present early stage of data protection where data users and the public are not fully aware of the issues, it is recommended that a statutory inspection report should always be shown to the data user in both draft and final form (except where there is a serious risk of tampering with the evidence), and that the inspection report should be made available to the public with only the minimum reservations necessary in view of arguments 3 and 4 above. The risks associated with argument 2 and 5 above should be accepted by the commissioning body, and with 6 faced bravely by the inspector.

The decision about the reservations in public disclosure should be made by the commissioning body, having heard the opinions of the data user and the organization.

6.8.6 Inspecting the Authority

The Authority is itself inevitably a data user, holding at least the following classes of personal data:

1. Personnel files of its own employees and control board.

2. Contacts within data-using organizations with which the Authority deals.

3. Particulars of aggrieved data subjects and other complainants.

4. Members of the public and public figures such as politicians, journalists, lawyers.

5. Data belonging to a data user which is held (perhaps only temporarily) for some legal or administrative purpose, e.g. inspection.

Some of this data will be of high sensitivity, and may be in a form which subjects it to legal requirements. The manner in which the Authority handles its own personal data is just as much a matter of public interest as that of other organizations, and should therefore be subject to the same rigor of inspection.

Some people will favour this requirement to submit to inspection as tending to ensure that inspections generally are not onerous to data users. Others, similarly, will fear that the Authority will be tempted to weaken the inspection for its own convenience. If inspections (contrary to the author's expectations) are commonly for good reason traumatic to data users, the Authority must resist internal pressures to weaken them.

To give confidence that the inspection of the Authority is carried out impartially, the inspector must be seen to have some independence of the Authority. Nothing which is said in section 6 implies that an inspector must be an employee of the Authority, and in the present case it is desirable that he should not be. Similarly, it is appropriate that the commissioning body for this inspection should not be the Authority, but perhaps some other department of state.

6.8.7 The cost of the inspection

There are many components of the cost of inspection:

1. Salary of inspector, and any supporting staff provided by the commissioning body.

2. Out-of-pocket expenses of inspector: travel, subsistence, etc.

3. Miscellaneous costs of inspector: stationery, phone calls, etc.

4. Working accommodation during inspection visit.

5. Organization's supporting staff during the inspection.

6. Organization's consumables cost: stationery, use of computer and other equipment.

7. Costs of disruption during the inspection.

8. Opportunity costs: losses because of actions not taken because of the inspection.

Not included in these is the cost of initial or consequential compliance with the regulations, which should not be incurred just because of the inspection.

There will also be some benefits for the data user and the organization from the inspection, including improvements to data quality, understanding of the workings of the system, and improved relations with the data subjects. There is evidence that these benefits can be substantial.

It is difficult to estimate what the nett cost of the inspection will be, but it must depend on the scope and strictness of the inspection and in some circumstances it will be heavy. This will generate pressures for the inspection to be made cheaper, if necessary by considerable loss of quality. There is evidently need here for a balance to be struck, and in the present limited state of knowledge of data protection inspection there must be an element of judgement. It would help if the actual costs of inspections were reported, so that informed decisions could be made in subsequent cases. The task of assessing the actual costs would be difficult, but might be added to the duties of the inspector.

For voluntary inspections, the cost will normally be shared within the organization in some agreed way. For statutory inspections, it is a matter of law who will pay for them, and the following considerations are relevant:

1. It appears inequitable to compel an organization to pay for an activity which may result in its own presecution.

2. Law enforcement is normally paid for by public funds.

3. Financial audits are paid for by the organization.

4. If an organization knows that it will have to pay for an inspection, it has an incentive for helping the inspection process to be efficient, in particular to save the inspector's time. Thus the general orderliness of the system, the quality of the documentation, and the extent to which it keeps clear of unnecessary data protection dangers would be all improved.

5. However, bearing the costs of a difficult inspection is a blunt instrument for penalising an unhelpful data user.

6. Some of the costs of inspection (e.g. numbers 7, 8 above) are difficult to quantify, and are therefore almost inevitably borne by the organization.

6.8.8 Determination of the regulations

The inspector will usually be asked to check a system's compliance, not with a specific set of regulations, but with "the law", by which the commissioning body may mean some or all of the laws which apply to the system. In simple cases, only a single data law may apply. In many cases, even for systems entirely within a single country, there may be several laws with independent and sometimes conflicting demands. Within international communities such as the EEC there is the possibility of overlapping national and international laws. Systems which are not entirely within one country may be subject to several national laws; even apparently local systems may receive some data from abroad, or send some of it there. Section 1 illustrates the profusion of transnational data traffic. It is to be expected that all these complexities will increase, at least for the next few years.

These conclusions may be drawn from this:

1. The inspector should be wary of accepting a commision which asks him to check compliance with "the law" in general.

2. A fully competent inspector would need extraordinarily wide knowledge.

3. To avoid dependence of such wide-ranging and complicated issues, an organization and an inspector would be wise to aim primarily at the generality of data protection principles (6.3), though they cannot entirely escape details of the law.

6.8.9 Relation to security

Privacy and security are often regarded as almost the same thing, and there is certainly a large overlap between them. There are seveal differences which are worth noting. Data protection is concerned with ensuring that (personal) data is used only in ways compatible with the interests of those concerned with it, as expressed in principles or regulations. Security is concerned to ensure that some facility (e.g. a computer) works as its owner requires and not to his disadvantage.

If an organisation has good security, it satisfies one requirement of data protection, namely restricted access to personal data. Other requirements, such as data quality, may be partly met. In practice, an organization which has good security is likely to have a businesslike approach to all its work, and this would provide a good base for data protection. But some requirements for data protection are not needed for security (e.g. notifying the data subject).

An organization which takes security seriously should have a person explicitly responsible for it. This person's rdsponsibilities could be extended to include data protection if its special requirements were noted. The requirements of security and data protection occasionally conflict (e.g. security may be increased by having numerous distributed copies of data, but privacy is diminished thereby), but can be reconciled in practice.

6.8.10 International aspects

The international dimension affects data protection at many points, and this section summarises its implications for inspection.

1. A system which is not located entirely within one country may be subject to the laws of more than one country (cf.6.8.8). Provided the regulations are well defined, this should not pose any new problem for the inspector.

2. A system which is widely distributed will generally be more difficult to inspect than one which is localised, for two reasons: firstly, inspection visits to more than one place may be needed; secondly, the transmission of data between the different points within the system by any means must be inspected. Both of these are more time-consuming and complicated if international factors are added to geographical distance.

3. For important international systems it may be necessary to include people of different nations in the inspection team. Such co-operation accords well with a widespread wish to harmonise data protection practice, but it may in the short term complicate the inspection.

6.8.11 Computer bureaux

The widespread use of other people's computers and other facilities for carrying out some or all of one's data processing affects the inspection. From the point of view of data protection inspection, the essential characteristic of a bureau is that it is part of a system, but not part of the organization. This has several consequences:

1. Legal and functional responsibility for the system is shared; there may be a clear division of responsibility, so that the inspector knows to which part a regulation applies, and to which part he must look for particular information, bu there may not, in which case the inspector's work may be complicated.

2. The powers of the inspector may not apply within the bureau as within the organization; in the case of statutory inspection, the regulations or the Authority may not cover the bureau; in a voluntary inspection, the commissioning body may have little power within the bureau.

3. The division of responsibility between the organization and the bureau poses problems for data protection, as there may be duties which are not accepted by either side, and inconsistencies and conflict between the two sides. The inspector must take account of these problems in his inspection.

4. The data user may be largely unaware of his responsibilities under the regulations; in extreme cases he may know lettle about computers and may not realise that the law applies to him.

5. Many computer bueaux are (for sound commercial reasons) run in a most business like manner: well organised, carefully documented, security-conscious, fully au fait with legal requirements, supportive of less competent data users. Such a bureau will save the inspector a lot of work.

6. It may be convenient to inspect at one time the work of several organizations who use the same bureau (the Swedish DIB spends a high proportion of its inspection effort on bureaux); for the purposes of inspection it is probably best to regard these as several distinct systems for which some of the information need not be gathered separately.

7. A bureau's list of data users may be a useful source of information, e.g. leading to data users who have not registered.

6.8.12 Non-standard operations

Data processing systems sometimes fail to work normally. When this happens, either the system stops, or unplanned alternative opeations take place, or planned alternative operations take place (or some mixture of all three).

The inspector should take an interest in these non-standard operating possibilities (which include start-up, testing, breakdown, maintenance, system change, standby, special running) for two distinct reasons. Firstly, the abnormal mode of working may violate the regulations. Even a stopped system could unfairly injure a data subject (if he has a right to expect some service from it), and, to the extent to which it frustrates the intentions of the organization, reflects badly on the organization. An improvised mode of working may sacrifice data protection principles to expediency; existence of a plannned alternative method of working indicates that the organisation takes seriously its responsibilities in operating the system.

If there is such a plan the inspector should examine it in the same way as he would that for the working system, so far as it is possible and to the extent to which he judges it to be necessary. If no plan for alternative modes of working exist, the inspector should attempt to assess the danger this presents to the observance of regulations: in a small simple system which is unlikely to suffer a substantial breakdown, has plenty of spare capacity and no sensitive data, the danger may be negligible; in a large, complicated, unreliable, fully-stretched system containing much sensitive data, it is intolerable. While realising that consideations of cost have a legitimate place in the drawing up of plans

(because the rights of the data subject do not completely overrule those of the data user), the inspector should not accept unforeseen accidents as a sufficient reason for the breaking of regulations.

Secondly, experience shows that non-standard operations often reveals unnoticed security weaknesses; a high proportion of detected computer crime, especially fraud, has been exposed during non-standard operation; and a disproportionate amount of computer crime occurs during non-standard running.

6.8.13 Sources of information

An inspector who wishes to maximise the amount of information he receives concerning a system must not restrict himself to what the organisation wishes to give him. There should be no question of it being unethical for an inspector to use any source of information about the system he is inspecting, due weight being given to its credibility. A high proportion of detected computer crime has been exposed initially because an insider decided to disclose improprieties. Subordinate employees

will often give a different, and in some respect more accurate, description of reality then those in charge. The inspector should attempt to ensure that subordinates can speak freely. Disgruntled ex-employees of the organization, aggrieved data subjects, the public in general should be encouraged in appropriate cases to give information, although much of it must be discounted as unreliable. However, it is no part of an inspector's job to encourage public expression of criticism of a system (e.g. in the media), which is effectively not inspection but punishment.

6.8.14 Inspecting databases

Sophisticated database systems of many sorts are becoming fairly common. ("Sophisticated" in this context means loosely that the data user does not understand how the data which he uses is stored and retrieved.) Such systems have several implications for the data protection inspection:

1. The definition of the "system" which is to be inspected may be unclear, as the personal data may be a small part of the whole, and the data users a small proportion of all users of the system.

2. The precise definition of the purpose of the system may be difficult, and the list of uses and users almost unmanageably big and constantly changing.

3. The levels of security, and of data quality with regard to accuracy and up-to-dateness, may be high, as they may be a central responsibility which are given great weight because so much depends on them.

4. Because such systems tend to be expensive, there is pressure to find new uses for existing data to help justify the cost.

5. Access to the data may be controlled by a central authority (the database administrator) so that a user cannot readily access data other than that which he is considered to need.

6. The software which controls the user's access to the data may be so complicated that the inspector cannot be sure that there are no loopholes permitting unauthorised access; indeed, the people who create and maintain the software must be able to bypass the normal barriers.

7. The data is stored in a complicated form such that useful access except by the normal software (and therefore subject to the central authority) is possible only for specialists.

8. For the same reason, a "complete listing" of the data, which the inspector might wish to examine for unauthorised entries, may be meaningless; such forbidden data could be distributed piecemeal in a way which would not be noticed.

9. Relatedly, data may be "erased" by destroying the link by which it is normally accessed, rather than by obliterating the data; such data may still be accessible by special means.

10 The boundary of a data subject's record may be undefined (5.4.2.2), as the database system may be able to cope with data chains containing any number of links, e.g. data subject's wife's mother's car's colour. Apart from the question of deciding how far along this chain the interests of the data subject run, there is the duty of not improperly disclosing data which refers to another person.

In this list are several at present unresolved problems, and in this respect the powers of inspection of sophisticated database systems must be considered incomplete.

6.8.15 Undisclosed systems

There has been public concern expressed (J1) that someone could operate a system outside a data protection law by taking care that it was not noticed (e.g. by ignoring a legal requirement for notification of the existence of the system), and thus avoid its being subject to inspection. The suggestion has been made that this is a serious danger which makes a nonsense of data protection laws.

Although it is strictly speaking outside the present study (which is concerned with inspecting the identified system), the problem of detecting undisclosed systems seems sufficiently near and important to deserve brief discussion here. Once again the risk analysis method (6.2.2) is helpful:

1. There must be a reason for the system being undisclosed. The evidence of the small number of published cases of abuse of personal data reveals commonplace reasons such as human error, laziness and cost-saving as much more important than the sort of sinister deliberate exploitation which could point an inspector to a small group of systems. However, motivation to abuse is mentioned above (6.4.2 item 3) as a factor conducive to inspection.

2. The undisclosed system must have the means to operate. The Swedish DIB has discovered many unlicensed systems (very few of them vicious) by inspection of computer bureaux which provided their means of operation.

3. There would have to be serious consequences flowing from the undisclosed system. The Swedish DIB largely relies on complaints to provide leads to objectionable systems. It has been remarked "If the abuse is concealed and has no effect, then it doesn't matter." (I1:qn.7) Without entirely accepting this (people may suffer without complaining effectively, and there may be a serious time-lag between the offence and the damage), one can recognize it as a practical philosophy.

It follows from this analysis that successful continuous operation of an undisclosed system requires that all three of these aspects fail to attract attention. The risk therefore appears small, but it is not negligible.

6.8.16 Length of inspection visit

Little has been said about the length of time which the inspector should spend in on-site inspection of the system. The Swedish inspectors usually allow about half a day (X1), even for a computer bureau on which many systems run (of course much more time is spent when it is considered necessary). The West German Federal Commissioner for Data Protection allows about ten times as much, and more on big systems (2.2.1.2.3). Computer security consultancy, which half overlaps data protection inspection, supports this larger figure.

Obviously these are qualitatively different inspections, with different aims and expectations. No doubt an Authority would vary its normal inspection strictness (6.8.2) if circumstances warranted it. The main conclusion to be drawn is that the judgement of experts of the appropriate scale of inspection shows wide variations, and that experience is not yet sufficient to justify dogmatism.

6.9 Acknowledgements and references

6.9.1 Acknowledgements

The following people gave much valuable material to section 6 of this report, but cannot be held responsible for any errors in it:

1. The working party on Privacy Audit, set up by the South West and South Wales Regional Committee of NCC:
   W.J.E. Evans (Ministry of Defence, Devenport) (Chairman),
   R.N. Essex (Imperial Group, Bristol),
   M.J. Holford (Yeovil District Countil),
   G.T. Morrison (Plessey Company, Beeston),
   H.H.W. Pitcher (NCC),
   L.R. Tallis (Bristol Polytechnic).

2. W.H. Buckley (Deloitte Haskins and Sells, Liverpool).

3. L.P. Waring (NCC).

6.9.2 References

B1 The British Computer Society code of good practice. BCS 1972. ISBN 0 85012 083 7

B2 F.M. Bancilhon and N.Spgratos: Protection of information in relational data bases: Proc. third International Conference on very large data bases, Tokyo, 3-8 October 1977.

C1 Canadian Institute of Chartered Accountant: Computer control guidelines (Toronto 1970), Computer audit guidelines (Toronto 1975).

D1 West German Federal Data Protection Act (January 1977)

E1 Council for Europe Resolution (73) 22. (Private Sector)

E1 Council for Europe Resolution (74) 29. (Public Sector)

F1 French Law Number 78-17 concerning data processing, files and liberties

F2 'Privacy Act implementation guidelines and responsibilites', Federal Register 40 (July 9, 1975).

G1 The Cost of Privacy, by Robert C. Goldstein (Honeywell Infoamtion Systems Inc., 1975)

H1 Records, Computers and the Rights of Citizens. U.S. Department of Health Education and Welfare. (O S) 73-94 (July 1973)

I1 Privacy - The Industry View (Institute of Data Processing Management 1979)

J1 "Data Protection Laws: The Real Threat" by Rory Johnstone (Computer Weekly 79-03-08)

L1 Report of the Committee on Data Protection (Chairman: Sir Norman Lindop), London HMSO. Cmnd.7341 (December 1978)

P1 Donn B Parker: Crime by Computer (New York 1976). ISBN 0-684-14574-X

P2 J.A.T Pritchard: Risk management in action (NCC 1978). ISBN 0-85012-180-9

S1 Swedish Data Act (1973: 289)

S2 Guidelines for the Data Inspectorate's inspection procedures in accordance with the Data Law (Swedish Data Inspectorate 1978) (In Swedish)

W1 L.P. Waring: Management handbook of computer security (National Computing Centre Ltd., Manchester, 1978)

W2 K.K. Wong: Risk analysis and control (NCC 1977). ISBN 0-85012-179-5

X1 Private communication from Swedish DIB

Y1 Report of the committee on privacy (Chairman: The Rt. Hon. Kenneth Younger), London HMSO. Cmnd. 5012 (July 1972)

Contents of this section

7.1 General observations

The EEC has been quick to realise the importance of information technology and its impact on the handling of personal data, as well as possible consequences for the individual and the Common Market. The whole area has been of such vital importance in social, political, economic and legal ways that an initial study of it seemed to be necessary. This was even more urgent, since the technical and regulatory environment was constantly changing.

To find out where to start and which way to take in this environment, this pilot project has been launched, with the hope of providing some signposts in the present confusion. But a framework for a long-range fundamental approach was also needed. With this double motivation, of providing a closer view of some present problems and forming a framework on which a systematic approach to the social, political and legal implications of data processing could be based, we selected, with the help of the Committee of National Experts, several topics which, separate from each other as they might seem, nevertheless turned out to be closely connected.

The chosen problems reflected main issues of debate at the beginning of this study, and drew attention to basic conflicts and structural problems on the level of

- the problem area
- the solution (regulation) area, and
- the economic environment.

On the level of the problem area, the issue of transborder data flow (section 1) was chosen both as being the starting-point of present international regulation activities and as being representative of one of the most contentious elements of existing legislation. Our main interest has been to arrive at a better understanding of this complex area and to find some criteria for structuring it. After a panorama of the most relevant environments in which this traffic takes place, we produced a classification according to the physical means of transmission, the people involved in it, the nature of the information transmitted, the nations involved, and the regulations applicable to this exchange. We have outline the enormous difficulties of obtaining quantitative data, but we have also identified possible ways of getting this data. Similar results were described for the measurement and evaluation of transborder data flows.

On the level of solution (regulation), we started from the present discussion on the practicability of certain data protection models and the proposals discussed by the European Parliament which have now become recommendations.

This led us to a closer look at the structure and practice of data protection agencies (section 2), and to questions of legislation (the natural person/other legal entity problem: section 3) and technical feasibility (right of access: section 5, control procedures: section 6).

With regard to the data protection agencies, we have been able to put together the legislative material on the environment in which these organisations have to operate and the evidence which we have collected on the practice which has already developed. From this evidence we have drawn conclusions about the political impact of these organisations and their possible role in international co-operation. We assume that these agencies deserve and will receive further study, both because it is in them that actual experience accumulates, and because of their importance for transborder data flow.

On the natural person/other legal entities problem, we have outlined major difficulties: ensuring that the intended protection is actually achieved, and defining exactly the scope of appropriate regulations. We have suggested that solutions for the first problem should be sought through business law, rather than from human rights which constitute the underlying values of the data protection discussion for natural persons. With regard to the seond difficulty, we have suggested that whenever

natural persons are in relevant contact with other legal entities, data protection regulations should apply. We have stated, however, that when these other legal entities are involved, there may be confusion with aims of data policy other than those of data privacy.

Regarding the right of access as one of the most important practical tools of data protection, we have looked into the technical feasibility and convenience of these rights in the light of technological advances. We have identified several elements of that right, and found that there is danger that some of these elements may have effects which are adverse to privacy and security, and that therefore any software or hardware to be developed for carrying out the right of access must take into account these risks, and should also reflect the nature of man-machine relations.

On the question of control, of whether compliance with data protection laws can actually be checked, we have tried to describe the basic notions of such procedures, and have arrived at some fundamental elements of such procedures which are independent of the regulation environment.

This has confirmed our general observation, that though solutions may differ in the particular approach according to legal, social and political traditions, a great likeness can be observed in the way in which industrialised states have set out to deal with the problems which information technologies pose for data privacy.

This is particularly due to the similarity in the economic environment, which we have analysed in section 4 in examining the economic problems caused by applying these technologies in these societies. We have concluded that the cost problem of data protection must be examined with greater care, since most of the assessments made so far are only speculations; and that there is considerable manoeuvering space for forthcoming international regulations.

So, although the areas selected may seem miscellaneous, they identify and analyse the most crucial points of information control in modern society, and present exemplary features of data protection both in its national and international environment.

But in the course of our observation we have come across further problems, partly arising from the points we have analysed, partly from the system in which they are incorporated. Before dealing with these consequences, we have a closer look at the infrastructure of this study itself.

7.2 Co-operation between the institutes

Co-operation on this study has been a valuable experience in the area of joint research. This positive experience makes us wish to enlarge the field of co-operation with other similar research institutes in the EEC. The multidisciplinary approach particularly, and the possibility of following research results in English, French and German, have proved most valuable for such a project.

In particular, one of the main objectives of this study was to create a basis for co-operation between the participating research institutes of the Community. In fact, even during the conceptual and contractual stages this project had been a joint effort.

Looking back now at these nearly two years of co-operation on the actual project and our research experiences, we believe that the wide-ranging approach outlined in 7.1 could not have been followed by one national research institute alone. This was not because of the means required, which were rather modest, but for deeper reasons:

First of all, the problems of information technology arise on an international level. So only by an

international research strategy could the different sources of information be made sufficiently available and be adequately accessed. Secondly, the multidisciplinary qualifications provided by the different institutes made it possible to look into these problems from different angles. Finally, the differences in the research environments and traditions have shown us that in spite of these national differences, similar means of approach to solving the problems are valid.

So co-operation was achieved, which both maintained national characteristics and yet joined in a common effort to produce a framework for analysing and evaluating the impact of information technology on personal data.

Positive though these experiences have been, there are still several items that we would like to see achieved in any further similar ventures.

One of the difficulties of such co-operation is that it demands a high co-ordination effort by the participating institutes. Though we think that by now an efficient substructure of co-operation between the institutes and the Commission has been achieved, it must be kept in mind that we have often been in a position where we had to follow legislatory and political events rather than to help prepare them, because of the time which would have been consumed in creating a structure for co-operation.

In future we would therefore favour an approach which provided results more fluently. We feel certain that we could then provide the Commission, as well as the Committee of National Experts, the member countries and other interested parties, with the kind of help which is needed during the preparation of decisions. We suggest that, if there are further activities of this type, means and organisational structures should be developed to give joint study groups more time to work together in the same environment, rather than only to meet occasionally.

Now that we know how to work together, we feel that the time has come to ask other research institutes within the Community who have similar interests to join further ventures. We believe this can only help to broaden and deepen the study.

On the basis of these deliberations and from our joint efforts, we offer some proposals for further research.

7.3 Further studies

Although data protection legislation has reached a stage of consolidation on both the national and the international levels, we still observe several issues which may become of crucial importance for the free flow of information in the Community and for safeguarding EEC citizens for whom national legislation was put forward:

1. Nations with data protection legislation can review it in the light of the experience of their data inspection agencies and public opinion. This seems to lead to the exemption of trivial data processing, and to easier procedures for the commonest data banks which contain data that does not seem dangerous. At the same time, a more careful approach is being made to specify sectors of data processing like public health, social security, employment agencies, research and national security. Among these sectors, all except perhaps the last deserve the attention of the EEC, since it is not altogether clear what consequences this more sectoral approach will have.

2. Though international regulations have been drafted, it is not clear when and how the different nations will respond to them, and how practical tney will prove in day-to-day data traffic. This is of especial importance with regard to data traffic between EEC and non-EEC countries. This uncertainty is partly due to

the circumstances that these regulations are mainly based on assumptions rather than conclusions. Here the actual practice and decisions of the data protection agencies on transborder data flow will be of vital importance.

3. The scope of data protection has grown widely in recent discussions. Issues like the balance of power, employment, national sovereignty, freedom of information, the 'New World Information Order' and economic dependency have been closely mingled with the former issues of privacy and openness. This enlargement of issues has led to controversies on data protection issues, and has widened the considerations for regulations to non-physical legal entities, as well as to economic data. The consequences of these complications for existing data protection regulation, and for the whole issue of information as an economic good have not yet been sufficiently analysed.

4. While regulation activities have reached some degree of consolidation, technological development has not stopped. It is still dubious how existing national and international regulations can react to new development like satellite communication and micro-computers.

5. In addition to existing regulations, there are still more far-reaching proposals for regulating information flows and giving undue protectionism that must not be ignored in further policy-making. This applies mainly to the recommendations of the European Parliament, but also to further activities of the Council of Europe in the area of access to government data. Whereas the former poses legal and organisational problems whose extent remains to be analysed, the latter may become important to present data protection regulations, and may pose problems of competition, as experiences with the U.S. Freedom of Information Act suggest.

6. Furthermore, the economic consequences of the drafted and proposed international agreements are far from being clear and demand further study.

7. Another issue which has been observed, but not explored, during the present study, is the influence of tariffs and regulatory aspects of telecommunications in the development of information flows.

These uncertainties on the one hand, and the experience with our interdisciplinary international research team on the other, lead us to suggestions for further research. We have identified the following research topics:

1. Technical problems of ensuring privacy, and data protection problems arising from new technologies

2. Data protection rights of the EEC citizen

3. Data protection and organisational policy

4. Possible role and structure of a European data protection control body

5. Economic aspects of harmonization procedures

6. Protection of research data

7. Transferability of data protection models

8. Assessment of information policy and legal problems with regard to telecommunications and data flows between EEC and non-EEC countries.

7.4 Acknowledgement

The authors of this study wish to thank all the numerous individuals and institutions who have helped with their free information and advice.