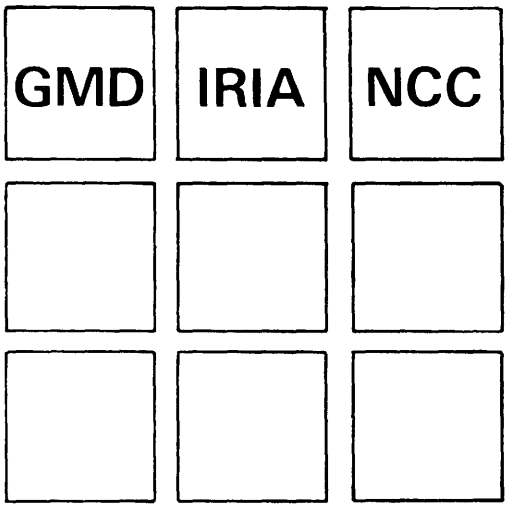


STUDY ON

DATA SECURITY AND CONFIDENTIALITY

FINAL REPORT

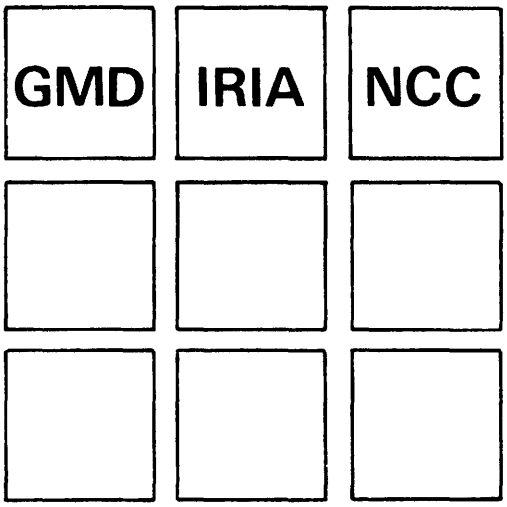
to the Commission for the European Communities

Volume 2 of 6

Section 2: Organization and method of operation of the data protection authorities

by H Burkert

JANUARY 1980



STUDY ON

DATA SECURITY AND CONFIDENTIALITY

FINAL REPORT

to the Commission for the European Communities

Volume 2 of 6

Section 2: Organization and method of operation of the data protection authorities

by H Burkert

JANUARY 1980

Contents of all volumes

Section 2 contents

2.2.1.2.1 Present legislative position
2.2.1.2.2 Data protectionlaw as a context for the Federal Commissioner for Data Protection and the Supervisory Authorities
2.2.1.2.3 Control authorities

2.2.1.3 Control authority for the Hesse Land Data Protection Law (HDSG)

2.2.1.3.1 Present legislative position
2.2.1.3.2 The Data Protection Law as a context to the control authority
2.2.1.3.3 Control authority

2.2.2 The Swedish data protection authority and its context of data protection law

2.2.2.1 Present legislative position
2.2.2.2 Data protection law as a context to the control authority
2.2.2.3 Control authority

2.3 Role and significance of the data protection authorities

2.3.0 Introduction
2.3.1 Analysis problems

2.3.1.1 Problems of comparability
2.3.1.2 Problems of classification and evaluation

2.3.2 Role and significance in the national sphere

2.3.2.1 Control authorities as a new type of administration
2.3.2.2 Functions of the control authorities
2.3.2.3 Political significance of the control authorities

2.3.3 Role and significance in the international sphere

2.3.3.1 Control authorities and trans-border data flows movement
2.3.3.2 International co-operation of the control authorities

2.4 Future demands on the control authorities in the European Economic Community and their feasibility

2.4.1 Recommendations of the European Parliament
2.4.2 Consequences

2.4.2.1 National control authorities
2.4.2.2 The European data protection body

2.5 Possible crucial points for future research

2.5.1 Crucial points within the subject of the enquiry
2.5.2 Related problems

2.6 Bibliography

2.0 Introduction

2.0.1 Definition of the item

From the broad framework of the decision of the Council dated 27.9.1977 (Official Journal of the European Communities Nr. L 255/25) -77/616/EEC- the Joint Study Group selected the question of the organisation and method of operation of data protection authorities.

The following criteria determined this choice:

(1) The demand for the harmonisation of data protection and data security in the European Community must, so far as one of its phases is concerned, take as its starting point existing provisions in the form of the numerous data protection laws and draft laws already in existence.

(2) The investigation of the provisions themselves is not sufficient. It is of decisive importance for manufacturers, users and data subjects, how the control regulations are implemented.

(3) The authoritative implementation agencies in the sphere of data protection are the data protection authorities for which provision is made or which have already been established in the various countries.

(4) The functioning authorities already have at their disposal experience in data protection practice, in particular in such important questions for harmonisation as the control of data traffic across frontiers.

(5) In addition the legal instruments used for harmonisation must be implemented by formal institutions. Experience in the national sphere can be applied internationally.

In view of the newness of data protection, and bearing in mind the resources available, it was obvious that this study could only represent a preliminary approach to the group of problems involved.

An additional point was that in view of the difficulty of carrying out this joint study and the continuing international development of this area, the definition of the tasks in this field would always have to oscillate between initiating policy and interpreting existing policy. Recent developments have been taken into consideration up to 1.9.1979. Owing to the technical demands involved in this international project, it was necessary to fix the closing date for publication relatively early.

2.0.2 Scheme of the report and methodological problems

To understand the data protection authorities, the legal background against which they operate is of decisive importance. In 2.1 we have therefore described this legal context in the various countries of the European community.

In the countries of Belgium, the United Kingdom and the Netherlands, which at the time of completion of this report still had no data protection law in force, we have described those drafts or reports of official committees on which public discussion has recently been focussed.

In the case of Italy and Ireland, we have contented ourselves with a reference to the fact that no generally accessible documents are available regarding the prospective control authority and its legal background in these countries.

We must refer here to a number of methodological difficulties regarding the description of the legal background for data protection control:

(1) Generally speaking, the legal provisions for data protection do not only cover those regulations which control the handling of protected information. For instance, the Federal German data protection law is

expressly understood to be a subsidiary law. Thus in the case of information conflicts between employers and employees, the regulations of the labour law have priority (see below 2.2.1).

(2) Furthermore, the method of operation of the data protection control authorities is not controlled by the data protection laws alone. The Danish data protection laws for instance (see below 2.1.2) refer to special provisions which are within the sphere of competence of a minister or of the government as a whole.

(3) In addition, the control institutions, as public and legal institutions, exist in a context of such legal provisions as are generally applicable for the establishment and functioning of such institutions, for instance laws governing employment and administrative procedure.

An adequate description of these organisations should therefore embrace all these manifold regulations.

Apart from these fixed provisions, in every legal code specific applications of the written law develop which can be grasped only by appealing to internal instructions, case law, etc.

And finally - and this is what makes comparison most difficult of all - all aspects of law are enshrined in a national historical legal tradition with which one becomes fully conversant - as with the learning of a foreign language - only as a result of long familiarity in use.

Against these difficulties - with which one is inevitably faced in making any comparison of legal systems - must be set the fact that the aims of the proposed legislation and the problems associated with it are structurally identical - at least for the countries with which the investigation is concerned. Differences do of course arise as regards the scope of these problems and the speed with which they arise. It is this almost identical starting point which makes a comparison of the legal context so attractive: the same problem is considered against varying legal backgrounds. The differing legal codes thus become equivalent to a social experimentation field, from which, as well as a study of the problem itself, lessons can be learned regarding the differing legal systems. (For example, trans-border data flow is one of the central problems of national data protection legislation. In Swedish legislation these systems are subject to a licensing obligation; in the German data protection law these systems are subject to a series of substantive requirements. Despite the differences - which will be examined in detail - it would

be possible to summarise the criteria laid down by both types of legislation for the permissibility of such systems, and to check each against the other for completeness. Any deviations could then be investigated to ascertain whether they were due to socio-cultural peculiarities or variations in political attitude, or whether there actually was a gap which might justify re-checking the regulations.)

A further reason for the significance of a comparative juridical study in this field is the fact that the comparative study of legal systems has explicitly played a part in determining the development of these legal fields in the sphere of data protection and computer legislation. Thus for instance the pattern of Swedish legislation is found to be repeated in a number of laws, whilst numerous reports of official committees have expressly referred to the provisions in other countries, and have taken these into account in their investigations. This development is being continued in the efforts of the Council of Europe, the OECD and the European Community, to reach mutually acceptable provisions by means of a process of comparative legal studies.

This contrast, between the limited nature of the approach by means of comparative legal studies and the necessity and practice of such a procedure, is manifested also in the problems which arise in describing the various national provisions.

Descriptions hitherto available are usually limited to brief descriptions in sequence or to tables in which miscellaneous items are often arranged in identical categories, without further differentiation. Only recently have a few differentiated descriptions become available.*

In view of these difficulties we did not wish to add to the existing descriptions any further ones limited to the data protection control institutions. In our opinion the problems of comparative legal study cannot be solved generally and absolutely, but only in the light of the particular need encountered for access to the knowledge stored - to be defined in each case - in accordance with which the data can be made available in a differentiated manner.

In this connection we started from the assumption that an essential function of the control authorities, in checking that the legal regulations are compiled with, consists of resolving conflicts between users and data subjects. In describing the legal background of the controlling authorities we have therefore restricted ourselves to the data protection regulations and asked only the following questions in relation to them:

*Cf. Bing, J.A., Comparative Outline of Privacy Legislation, Comparative Law Yearbook Vol.2, p.149 ff.

Points of interest to users:

1 Which type of data is covered by the particular data protection legislation under consideration (type of data)?

2 What type of data processing is covered by the data protection legislation (type of data processing)?

3 What formalities must be respected in implementing an information system (prior conditions for data processing)?

4 What obligations must be complied with in the data processing (obligations of the user)?

Points of interest to the data subject

What rights can the data subject exercise and at what costs (rights of the data subject)?

This series of questions seems to us adequate in the first place to evaluate the particular national data protection legislation in question, in relation to the clash of interests which constitutes the milieu in which the control authority is operating. These questions will

therefore be worked through first in respect of each country.*

As part of the descriptions of the position in the different countries the evaluation of the particular control authority - as an initial approximation - then follows.

This evaluation is made on the basis of the answers to the following questions:

(1) How is the particular institution integrated with the remainder of the country's institutions?

(2) How is the institution constituted?

(3) What are the tasks of the institution?

(4) What resources are available to the institution for carrying out its tasks?

The description and also the summing up (2.3 and 2.4) involve ideas from the field of organisational sociology. For various reasons however it is not intended that the present report should be understood as such a sociological analysis:

*The public sector is included as far as is necessary for understanding the working of the data protection authorities.

(1) The use of a methodology derived from the sociology of organisations tends to neglect the legal context in which the organisations have to operate.

(2) Such a methodology could be extended to investigate the sociological effects of legislation.*

(3) No such adequate methodology is yet available; to develop it would have exceeded the resources of the project, as the present investigation is essentially a first approach to this international complex of problems. Essentially we can only define the problems.

*Here future tasks would arise in the course of the investigation of the long term results of information technologies in an industrial society, in particular regarding the possibility of investigating the problem of control in the highly developed industrial societies. Such effects would be of particular importance in connection with the question of how information systems encroaching across frontiers might be controlled, say in accordance with the aims of the European Community - in this connection see below suggestions for further investigation: 2.5.

At the present time it also seemed that there was little point in burdening institutions which are only at a formative stage with time-consuming subsidiary investigations. In the long term however these institutions should prepare themselves to become the object of socially important research. Preparations and the legal arrangements necessary for them should facilitate such access to these authorities. In this respect the Swedish authority, which makes provision in its budget for such work, is a model of the way in which the wider use of modern technologies can be encouraged.

We therefore regard it as our duty to describe the data protection authorities, so as to ensure that the problems arising from their action and interaction in the interplay of interests in national data processing, private data processing and the data subject are clarified. This will permit a realistic assessment of their possibilities within one country and their contribution to a possible harmonisation of the European Community regulations. It will also make it clear where future investigations should begin.

We have described the data protection systems of the German Federal Republic and of Sweden separately and in particular detail (2.2). The system of the Federal Republic was deliberately selected because of its complex

structure, whose federal nature is particularly relevant to the problems of harmonisation. The Swedish system was selected because of that country's long experience.

This description is followed by an attempt to analyse the role and importance of the authorities (2.3): after some introductory remarks on the problems of such an analysis, the main functions of the authorities, both in the national and international sphere, will be described.

These functions will, in 2.4, be compared with the requirements derived from the recommendations of the European Parliament. This section also contains our conclusions regarding further steps of harmonisation.

The concluding section (2.5) contains a survey of further research activities which, in our opinion, seem necessary as a result of this preliminary study.

The bibliography (2.6) includes not only the titles to which reference is made in the footnotes, but also the literature which seems to us authoritative in the field covered by this investigation, and should therefore provide useful information on this range of subjects.

2.1 Control authorities seen in the context of national data protection laws and draft laws of the European Community

2.1.0 Preliminary remarks

The control authorities for data protection are described below in the context of data protection law, so far as this has already been developed or is defined in generally accessible draft laws or from reports of official committees.

The control system of the Federal German Republic will be described separately, together with the Swedish system, in 2.2. This separate treatment and the inclusion of Sweden in the same section seemed to us desirable, as these two countries have had the most experience in the implementation of data protection rules. Furthermore, they are typical examples of the practical application of two different philosophies of control.

2.1.1 Belgium

2.1.1.1 Present legislative position

Although a number of individual statutes already protected the private sphere in the fields of both civil and public law, at the beginning of the seventies it was fairly generally accepted that a fresh law was required for the protection of the private sphere in order to keep pace with the latest technological developments. Since 1970 there have therefore been numerous initiatives both on the part of the Government and of members of the Legislature to put this matter right.

One of these drafts, the so-called "Vanderpoorten" draft, appeared to us the most thoroughly worked out, and is at present taken as a basis for discussion in Belgium.* The draft was made in 1976. The basis of this description is the original text in its French form.

The draft deals with the danger to the sphere of private life by technical means in general, and with the dangers from data banks in particular (chapters III and IV). Reference is made to these chapters below.

*See "Banque de Données, Enterprises, Vie Privée" Data Bank, Business Undertakings, Private Life; Conference Proceedings; Namur 1979.

(Belgium)

2.1.1.2 Data protection law as a context to the control authority

Types of data

Protection is extended to data concerning natural persons and corporate bodies, including data from which a particular person can be identified either directly or indirectly. (The problem of corporate bodies is further discussed in section 3.) The inclusion of corporate bodies in these arrangements does not nullify their obligations in accordance with other laws to make some matters public.

Some kinds of data, the so-called "sensitive data", are subject to special requirements. They may only be processed in accordance with legal regulations or with the express consent of the person affected. Such data are details of race, personal opinions, or activities regarding: trade unions; co-operative societies; cultural, philosophical or religious questions. Membership lists held by such institutions are exempted. Data regarding social insurance and health (with the exception of collections of data in the possession of the particular doctor concerned) are also considered sensitive.

(Belgium)

The same applies to data from the field of penal proceedings: such data may be compiled only by authorities in accordance with their statutory duties.

If the authorities in this connection have only limited criminal jurisdiction (such as for instance the price control authorities), they may collect such data only if the person concerned or the control authority (see below) have agreed, or if this is permitted by a relevant law. Similar restrictions apply to private institutions operating as credit information bureaux.

Types of data processing

The central feature is data processing in data banks. According to the definition of the draft, a sensitive data bank is an organised collection of data of any kind, which contains data of the above kinds relating to persons, which has been prepared for the purpose of automatic data processing, or which has been prepared with the help of automatic data processing. It also includes manual data processing, if this is connected with automatic data processing.

(Belgium)

Territorially, all data banks in Belgium are covered, irrespective of the nationality of the operator. Data banks of supranational organisations, such as the EEC, are however not subject to Belgian jurisdiction.

The following are excluded: data banks by means of which corporate bodies fulfil their duty of publication, and the data banks of the National Statistical Bureau, except for Government research purposes.

Conditions on which data processing is permitted

Data banks in the private sector (and also data banks in the public sector which have not been compiled in accordance with a law) must, before being put into use, either be registered with the control authority or licensed thereby.

Only registration is required for data banks whose data:

- are processed only with the written permission of the data subject; or
- (in the public sector) are processed by the competent body as part of its legal duties;

and

- which do not contain any sensitive data (see above).

(Belgium)

The control authority may, as far as necessary, issue special operating instructions, for instance to control the transmission of data to third parties, and may grant release from certain obligations (see below), e.g. from the obligation to provide information.

All other data banks are subject to the licensing system. After submission of an appropriate application, the control authority grants permission which contains obligatory operating instructions regarding:

- the purpose of the data bank
- the relevance of the data to the purpose of the data bank
- the methods of compilation of the data
- the methods of automatic data processing
- the transmission of data to third parties
- the data security systems
- the period of use of the data.

The control authority may in addition regulate:

- the type of automatic data processing system selected

- the rights of the data subject (see below).

(Belgium)

All alterations require the prior consent of the control authority.

Duties of the user

The operator of the data bank (who may be a legal or a natural person) must designate the person responsible for the data bank, irrespective of whether he performs the data processing operations on his own behalf or for other people. This responsible person must be directly subordinate to the operator.

In addition the operator must make the necessary declarations for the initiation of the licensing or registration process. He must then make sure that the operating instructions and legal regulations are observed. He must ensure that the quality of the data is maintained and that the data processing staff comply with the instructions and regulations.

Rights of the data subject

The data subject receives from the responsible data operator information regarding the initial storage of his data, together with information regarding the rights available to him. (This process may however be varied by the control authority in accordance with the operating instructions.)

(Belgium)

The data subject has the right, once a year, within thirty days of requesting it, to receive information on the following points:

- what data regarding him are stored
- for what purpose the data are being processed
- which third parties have received data regarding him during the last year.

The right to such information may be repudiated by law, by a decision of the control authority, or by a decision of the competent medical professional association. The data banks of the criminal prosecution and safety authorities are also exempt.

The data subject may, in the event of a refusal on the part of the operator to erase the data or correct them, apply to the "Courts of first instance" if he considers the data incorrect or irrelevant. The courts may even order the destruction of irrelevant data. Third parties who have received such data must be informed by the operator of any alteration.

(Belgium)

2.1.1.3 Control authority

Incorporation

The control authority is an independent authority, initially financed from the budget of the Ministry of Justice; the authority should subsequently finance itself from the charges it levies.

Structure

The authority (Office de Protection de la Vie Privée - Board for the Protection of Privacy) consists of a Supervisory Council (Conseil de Surveillance) and an Inspection Commission (Commission d'Inspection). Each body consists of two chambers, each with three members appointed by the Crown in consultation with the Legislature and the Executive. The composition of the bodies must reflect the political majority relationships.

Each body shall draw up its own procedural rules and appoint its own staff.

The authority shall publish a tariff regulating its fees.

(Belgium)

Tasks

The task of the Supervisory Council is to rule on complaints made against the Inspection Commission. The other tasks of the authority are generally carried out by the latter.

The control authority carries out the registration and licensing process. In doing so it must respect time limits prescribed by law.

In the public sector it must in addition express its attitude to draft laws for the institution of data banks, which are then to be exempt from the said procedure. The views of the authority will be published and recorded.

The authority will make it its business to deal with complaints from the public, and on its own initiative. Complaints must be decided within a period of two months.

In addition the authority shall keep a generally accessible register of registrations and licences. This register shall contain:

- the name of the responsible person
- the purpose of the data bank and the nature of the data to be processed therein
- the groups of persons who may have access to such data, and
- the date of registration or licence.

(Belgium)

Powers

If in the operation of the data bank danger to privacy or unfair discrimination is found, the authority shall be empowered to alter or revoke permits.

In addition the authority has the necessary rights of access and examination.

2.1.2 Denmark

2.1.2.1 Present Legislative Position

Data protection in Denmark is controlled by two laws:

1 The law regarding private data banks (Lov om private registre, Lov nr. 293. This law will be referred to below by the abbreviation "PRA", in accordance with the English translation "Private Registers Act").

(Denmark)

2 The law regarding data banks held by public authorities (Lov om offentlige myndhigeders registre, Lov nr. 294 - this law will be abbreviated to "PARA", in accordance with the English translation "Public Authorities' Registers Act").

Both laws were passed on 8 June 1978 and came into force on 1 January 1979, although the application of a series of regulations was postponed until 1 January 1980, in accordance with transitional provisions.

The basis of the description is the English translation of the Danish text authorised by the Danish Ministry of Justice (OECD Document DSTI/ICCP/79.11/05).

2.1.2.2 Data protection law as a context to the control authority

General preliminary remarks

The Danish system of data protection is essentially oriented towards substantive law. In the private sector the regulations are specified to particular fields, in the public sector they are arranged according to the various phases of data processing. There is no general registration or licensing obligation in the private sector.

(Denmark)

Types of data

Protection is extended to all personal data which are electronically processed. Personal data are data relating to natural persons or corporate bodies which are identifiable; they are still deemed to be identifiable even if knowledge of a personal identity number or similar means are necessary.

Personal data, stored in non-automated systems, are only protected in the private sector, and only if they are of a nature which - irrespective of whether they are of a private or commercial sort - can reasonably claim protection against general publication.

Special protection is due to sensitive data, i.e. data regarding race, religion, health, drug dependency, political views, sexual behaviour and criminal record. In the private sector such data must not be stored or transmitted, unless this is allowed by another law or the data subject agrees or must assume owing to circumstances that such data will be stored. In the public sector the recording of such data is allowed, but only if they are relevant for the particular purpose of the data bank. Political data, unless they are generally accessible, must not be stored.

(Denmark)

In addition data is exempt from data protection if it is stored solely for scientific or statistical purposes or for the purpose of biographical or similar research. In the case of sensitive data, exemption is allowed only for health data or for scientific or statistical purposes.

In the public sector data banks kept for police and military intelligence purposes are also exempt.

Type of data processing

As is clear from the above, the whole field of electronic data processing is subject to the data protection law; manual data processing is included only if it takes place:

- in the private sector, and
- systematically, and
- with the above types of data.

Conditions in which data processing is permitted

The requirements in connection with the implementation of information systems are in the private sector essentially of the nature of substantive law, with the law for various fields of utilisation being provided with different regulations. It distinguishes between commercial undertakings, credit information undertakings, direct mail agencies, and service bureaux.

(Denmark)

The following requirements apply to general commercial undertakings, i.e. those which do not come within the special categories mentioned:

Commercial undertakings may record and transmit protected data only so far as this is a component part of the normal activity of these undertakings. In addition, it is forbidden to maintain "blacklists", unless they are specifically authorised by the data protection authority - in which case the regulations covering credit information bureaux shall apply.

Further limitations on the recording of data may be provided by the Minister of Justice after consultation with the data protection authority; in this connection he may in fact specify the application of the regulations for credit information bureaux (see below) to particular types of data bank or particular types of data. In the field of communications a series of special provisions apply which mainly relate to the quality of data. Data which have been recorded for longer than five years must not be communicated.*

*There are however again three exceptions to this time limit; they may be communicated if the party affected has agreed, if they are for the purpose of clarifing facts of paramount importance, or if another legal provision permits such communication.

(Denmark)

Special requirements apply to the management of credit information bureaux, direct mail agencies and service bureaux.

Credit information bureaux are undertakings which record data regarding the financial strength and the credit-worthiness both of natural persons and of corporate bodies, making these available to third parties.

Before starting its activities, such an undertaking has to apply for registration with the data protection authority; as soon as this initial duty of registration has been fulfilled the undertaking can start its activities.

In this field also the principle of necessity applies as a basic requirement for the recording of data. Sensitive data are to be excluded from such recording. The Danish legislature has created a further type of "sensitive" data especially for the field of credit information: data according to which the credit-worthiness of a particular person is questionable: the recording and use of such data is permissible only for five years, unless they are of overwhelming importance for clarification of the financial strength and credit-worthiness of the person in

question. The law expressly permits the recording of data such as names, addresses, professions, trades or data which are available from public sources. Data which are neither sensitive, nor included in the categories just mentioned, may be recorded if the data subject is informed thereof; such notification must be given with a period of four weeks after first recording and must contain a reference to the right of the data subject to be informed. The Minister of Justice may exempt credit information bureaux from the obligation in question by a decision, which must be announced in collaboration with the data protection authority. The communication of data is also subject to the principle of necessity. Sensitive data may not be communicated. Data which have direct reference to the financial strength and credit-worthiness of a person may only be transmitted in writing. Publications of a credit information bureau may contain data only in summarised form, and may only be communicated to customers of the bureau; furthermore, such publications must not contain the personal identity number. Whole sets of records may only be handed over or communicated to credit information bureaux which are also registered; such communication must be notified to the data protection authority.

(Denmark)

Direct-mail agencies are undertakings which handle addresses of groups of persons, companies, societies or undertakings or address envelopes on behalf of third parties, or despatch literature which is intended for the above-mentioned groups.

Direct-mail agencies may only record quite definite types of data; these recordable data are listed below:

- name, address, profession
- data which are freely available from Danish commercial registers
- data regarding leisure interests and similar details.

The recording of sensitive data is not allowed. This strictly circumscribed framework of recordable data may be still further restricted by a decision of the Minister of Justice.

The communication of membership lists of societies by direct-mail agencies and the use of the lists on behalf of third parties is only possible with the agreement of the association concerned.

(Denmark)

Service bureaux are undertakings which process data on behalf of third parties by means of EDP. They are obliged to apply for registration with the data protection authority before starting their activities. In carrying out its activities the undertaking is bound by the conditions of its agreement with its customer.

Duties of users

Commercial undertakings are obliged to erase all data or correct them if this is requested by the data subject. Applications to this effect must be answered within a period of four weeks. If the undertaking does not comply with these obligations, the data subject may apply to the data protection authority, which has the legal power to require the undertaking in question to comply. Moreover the data protection authority has the power to oblige the undertakings to inform all parties to whom the data which is now to be destroyed or corrected have been communicated in the last six months; and to inform the data subject of all such parties.

For records handled by EDP, these obligations are in some cases modified; data which is contained in such records and has lost its significance for the purposes of such recording must be destroyed.

(Denmark)

To prevent false or misleading data from being stored in these records, undertakings are obliged to introduce a checking system. If with the aid of these checking procedures, data are found to be false or misleading, they must be erased without delay. To prevent misuse of the stored data, undertakings are obliged to take the necessary security measures for EDP data banks.

Special duties exist for the various special categories of information systems:

For general commercial undertakings, when false or misleading data have been communicated, there is a duty to inform the party concerned and all other parties who have received these data; moreover the data subject must be informed of all parties which have received these false or misleading data. Credit information bureaux are under obligation by law to erase or correct all data which are found to be false or misleading. Direct-mail agencies are under obligation at the request of the data subject to destroy all data which refer to him. The initiator of mailshots is also obliged - unless he is identical with the address-list publisher - to pass on any request for deletion of an address to the agency in question. Service bureaux may, as explained, use data

only for the purpose laid down in the contract. To prevent misuse of the recorded data, they are obliged to introduce any necessary security measures.

Rights of the data subject

In the private sector the data subject has in general:

- a right to be informed
- a right to erasure or correction of data, and
- a right to complain.

In the sphere of credit information bureaux, the data subject has an automatic right to be informed in those cases in which data are recorded for the first time, which are not publicly acessible; at the same time he must be advised of his right to be informed. Furthermore he may demand to be informed of all data which the bureau has communicated to third parties in the last six months, and regarding all data concerning himself stored on index cards, punched cards or other media; furthermore the bureau is obliged to inform him of all other types of data which concern him; he also has the right to examine the records of the bureau. He may demand that the notifications be made to him in writing. He cannot

however ask to know the source of the recorded data, and he has to pay a fee for written notification of the data, such fees being laid down on a uniform basis by the Minister of Justice. The data subject may demand the erasure or correction of data which have been found to be false or misleading or which should not have been recorded or communicated. In the event of refusal of his request, the data subject also has the right to complain to the data protection authority.

In the case of address-list agencies the data subject may only demand that his data be erased at his written request. This applies irrespective of whether he addresses his application to the address-list agency itself or to the agency's customer, as the latter, as explained, is under obligation to pass on the request.

In the case of service bureaux, the rights of the data subject relate directly to the undertaking's customer.*

*In the public sector the data subject has the right to be informed of data which concern him as soon as possible. In the special instructions for the individual systems (see above) this right may be modified.

(Denmark)

A modification applies to medical data. In these cases the data subject, together with his doctor, has to make a suitable application; the data will then be passed on to the data subject via the doctor treating him.

The general claim or right to be informed may be overruled by sufficiently strong public or private interests; this may apply either to the whole or to only part of the data requested.

Furthermore, the data subject has no right to be informed of data which is stored solely for statistical purposes. Finally, in the public sector, the right to be informed may be exercised only once within twelve months, although exceptions to this time limitation may be justified by special interests.

Disputes regarding the exercise of the right to be informed may be submitted by the data subject to the data protection authority.

(Denmark)

2.1.2.3 Control authority

The necessary supervision to ensure that the data protection regulations are observed, both in the private and in the public sector, is carried on by a data surveillance authority (abbreviated to "DSA" in what follows).

The provisions regarding structure and allocation of function in the DSA are laid down in the PARA; the intructions regarding the duties and rights of the DSA are to be found both in the PARA and also in the PRA, according to the different fields concerned.

Incorporation

The DSA is an independent authority. Its budget is separately shown in the budget of the Ministry of Justice and for the first year amounted to 2.5 million Danish kroner.

Structure

The DSA consists of a Council and a Secretariat.

The Council consists of a President, who must have the qualifications of a judge, and six other members.

(Denmark)

The co-operation between the Council and the Secretariat is regulated by an order of the Ministry of Justice.*

The Council is appointed by the Minister of Justice; the period of service is four years.

At present the Council consists of scientists, representatives of the administration, the press and manufacturers.**

At present the Council meets approximately every month and decides questions of principle which are submitted to it by the Director of the Secretariat.

The Secretariat, under the management of a Director, attends to the business of the data protection authority arising from time to time.

The Secretariat at present consists of a legal and a computer-oriented department. At present the Secretariat comprises twelve people. An increase to 25 is planned.

*Details are laid down in the communique of the Minister of Justice no. 160 dated 20 April 1979.
**The members are however appointed as individuals, not as representatives of these groups.

(Denmark)

Tasks

In the private sector the DSA has the task of ensuring that the compilation and operation of data banks complies with the legal provisions of the PRA and the instructions issued in accordance with the PRA; it has to carry out this task either at the request of a data subject or on its own initiative. This general task is specified as follows:

- The DSA must maintain a register of credit information bureaux and service bureaux.
- The DSA must deal with the complaints of data subjects, and take appropriate steps.
- The DSA must express its views when the Minister of Justice wishes to modify the sphere of application of the laws.
- The DSA decides the permissibility of the compilation and electronic processing of sensitive data outside Denmark.

The decisions of the DSA can be challenged only in the competent courts.

(Denmark)

At present the main task of the DSA is to acquire a comprehensive picture of the data processing position in the private sector. In addition, the drawing up of data security regulations for credit information bureaux (at present about 12) and service bureaux (at present about 80) has been begun. Blacklists (at present about 12 are known) are also being checked; their maintenance - as already explained - requires the approval of the DSA.

In the public sector the DSA has the basic task of supervising all data banks to which the PARA refers. In particular this task includes the duty of making sure, either on its own initiative or on the basis of a complaint, that the compilation and the operation of a data bank is in accordance with the legal requirements of the PARA and other directives. As in the private sector, certain tasks of the DSA are specifically mentioned:

- it must express its views when the Minister of Justice wishes to extend the field of application of the PARA
- it must express its views when the compilation or amalgamation of data banks in the public sector has to be approved, the regulations regarding the structure and method of operation of the data bank have to be issued

(Denmark)

- it must settle disputes regarding the right of access
- it must report every infringement by public bodies to the responsible authority and the competent Minister
- it must submit to the Danish Chamber of Deputies an annual report on all its activities, which will be published.

On 1 July 1979 the time limit expired for the preparation of draft instructions for the public sector systems (at present about 600). Some of the sets of instructions (which in some cases are very detailed) have already been issued by the various competent Ministers in collaboration with the DSA.*

The DSA plans to append to its first annual report a summary of the data banks in the public sector, which will help data subjects to find out which sets of instructions apply.

*In the case of difficult systems the PARA provides for the deadline to be extended.

(Denmark)

Powers

For the fulfilment of its tasks, the DSA has the following rights in the private sector:

- It is entitled to demand and examine all data which are necessary for the fulfilment of its tasks.
- The members of the DSA are entitled to be admitted to all installations and premises which are concerned with data processing.
- The DSA is entitled to prohibit the unlawful recording and communication of data, and to order the erasure of data banks which are not conducted in accordance with legal regulations.
- It is entitled to order the erasure or correction of data, particularly in cases in which data were recorded before the PRA came into force.
- It is entitled to prohibit certain processes for the collection and communication of data if the corresponding process inherently involves a considerable risk, in the opinion of the DSA, that false or misleading data may be recorded or communicated.

(Denmark)

- The DSA is entitled to oblige an undertaking to take certain control and security measures to prevent the risk of the creation of false or misleading data or the misuse of data due to access by unauthorized persons.
- The DSA has the right to determine the form and the content of legally required reports and applications.

In the public sector the DSA has the following rights:

- Its members are entitled to be admitted to all installations and premises which are concerned with data processing by the appropriate authorities.
- The DSA is entitled to suggest extensions to the individual directives.
- It is entitled to publish its comments on the agreements and directives.

2.1.3 France

2.1.3.1 Present legislative position

The French data protection law was passed on 6 January 1978.* The following description is based on the French original.

2.1.3.2 Data protection law as a context to the control authority

Types of data

Protection is extended to personal data referring to natural persons. Within the meaning of the law, data are regarded as "personal" if the identification of the natural person to whom the data relate is possible, directly or indirectly.

Personal data relating to criminal records and/or security mesures may be processed only if this is permitted by law.

*Loi no. 78-17 du 6 janvier 1978 relatif à l'informatique, aux fichiers et aux libertés - J.O. 1978 p.227.

(France)

The processing of so-called sensitive data is forbidden in principle; these are data regarding race, political opinions, philosophical or religious views and the membership of trade unions. Exceptions to this prohibition of processing are provided for in three cases: if the data subject has given his consent to the processing of the data which refers to him, if the said data are stored by religious, political, philosophical or trade union groups concerning their own members, or if the public interest in the processing of the sensitive data takes precedence over the individual interest; the latter exception requires a decision on the part of the French control authority and the Conseil d'Etat.

The press and audio-visual media are not excluded from the processing of sensitive data; but existing regulations for the media apply to this.

Types of data processing

The law covers all personal data processing. "Data processing", within the meaning of the law, means all of the processing steps which are carried out by means of automatic processes and relate to the collection, storage, alteration, retention and erasure of personal

data. Regulations referring to data collection, data security, and sensitive data, apply to non-automated as well as automated systems.

Conditions on which data processing is permitted

The law provides a standard and a simplified approval process for both the public and private data processing sectors.

Standard approval process for the public sector

Except when data processing by public bodies requires legal authorisation, the data processing applications of these bodies are approved, after a reasoned opinion from the Data Protection Commission, by an administrative decision.* For this purpose the public body in question must submit an application for opinion to the Data Protection Commission; this application must specify in detail:

*Public bodies within the meaning of the law are the authorities, the public welfare institutions, the district corporations and the corporate bodies constituted in accordance with civil law which carry out public tasks.

(France)

- the person applying, and the person who is responsible for the decision to adopt data processing, or, if he lives abroad, his representative in France
- the nature, purpose and, where necessary, a description of the processing
- the department entrusted with the execution of the data processing
- the department where a data subject's right of access may be exercised, and the measures taken to facilitate the exercise of this right
- the classes of persons who for functional or organisational reasons have direct access to the stored data
- the personal data processed, their sources and retention periods, and the recipients or classes of recipient who are entitled to receive these data
- the combination, interlinkage or any other form of correlation of these data, and their communication to third parties
- the measures taken to ensure the security of the data processing and of the data, and the protection of legally protected secrets
- any intended transfer of data abroad.

(France)

All private natural persons or corporate bodies, who neither belong to Government nor regional institutions nor carry out public tasks in civil law, are under obligation to give notice of the intended use of data processing to the Data Protection Commission. The notification must contain the same details as are laid down for the opinion procedure in the public sector (see above); in addition the notification must also contain an assurance from the private data processor that the data processing will comply with the provisions of the data protection law.

On receipt of acknowledgment from the Data Protection Commission the data processing can be put in hand.

For the commonest forms of data processing, in both the public and private sectors, a simplified procedure is provided. In this procedure, the data processor need only make a declaration to the Data Protection Commission that the regulations drawn up by the latter for the field concerned (cf. in this connection 2.1.3.3 below) will be respected. On receipt of the acknowledgment from the Commission, the data processing work can be put in hand.

(France)

Duties of users

Besides the obligation of the user to specify the type and content of the data processing in the application, which has already been described, the law imposes on both public and private operators duties regarding:

- collection
- storage
- informing the data subject
- the correction of false data, and
- security of the data against access by third parties.

The collection of data must not take place using fraudulent, illegal or unfair methods. When data is collected, information must be given regarding:

- whether answers to the questions are obligatory or voluntary
- the consequences of failure to answer
- the recipients of the collected data, and
- the procedures for the right of access and the correction of data.

(France)

If the questions are asked by means of questionnaires, these must contain this information.

These provisions do not apply to criminal prosecution authorities.

Sensitive data must not be stored without the express agreement of the data subject. Exceptions to this principle apply only to lists of members of philosophical, political or trade union groups held by such groups, and for the storage of sensitive data which is justified in the public interest.*

Data regarding criminal acts, sentences or security measures may be processed by the authorities concerned with the administration of justice, and by other authorities as part of the fulfilment of their legal duties, and also by corporate bodies constituted under civil law, which perform public duties, on the basis of a report justifying this from the Data Protection Commission.

*In the latter case however, a suitable decree from the Conseil d'Etat must have been issued, supported by a proposal or an opinion prepared by the Data Protection Commission.

(France)

Storage of other personal data may be carried on only for the period described in the notification or the application for a decision. Storage beyond this period can be permitted only by law or a decision of the Data Protection Commission.

The data user must inform the data subject of all data which refer to him.*

At the request of the data subject, the user must undertake correction, completion, explanation, updating, or erasure of such data as are incorrect, ambiguous, incomplete or out of date. After the alteration has been made, the data subject must be provided, free of charge, with a copy of the corrected data. The onus of proof of the correctness of the data stored, when the data were supplied neither by the data subject himself nor with his agreement, is on the user.

As soon as the user learns of the incorrectness or incompleteness of data in a personal data file, from any source other than the data subject, the data in question must be corrected.

*In this connection, see below under "Rights of the data subject".

(France)

If incorrect data has been supplied to a third party, the latter must be informed of the correction of the data.

Each user is under obligation to the data subject to take all appropriate precautionary measures to ensure the security of the data, and to prevent them from being falsified, damaged or made accessible to unauthorised third parties.

Rights of the data subject

The data subject has a right to be informed and a right to request corrections.

The data subject has a right to be informed, which can be exercised against all data processing departments. On request he can learn whether, and if so what, data had been stored about him. The enquiry must be accompanied by the appropriate fee, which is fixed by the Data Protecion Commision.

If the data subject believes that data are being withheld from him, he may apply to the competent court.

Medical data may only be communicated to the data subject through a doctor whom he nominates.

If the person concerned requests information regarding data which are of interest for state security, defence of the country or public safety, he must address his request for information direct to the Data Protection Commission.

The data subject may demand:

- Correction,
- Completion (amplification),
- Explanation,
- Updating,

- Destruction of data which are incomplete, ambiguous or out of date, and/or which should not have been gathered or processed.

In the event of refusal, the onus of proof is on the user, unless the data subject himself has given the data in question or the data have been stored with his consent.

The fee must be returned in the event of a justified complaint.

2.1.3.3 Control Authority

Incorporation

The Commission is an independent administrative authority. F1

The fincancial resources necessary for the fulfilment of its tasks are made available in the budget of the Ministry of Justice.

(Footnote 1: The Data Protection Commission is abbreviated to CNIL in what follows, in accordance with the French designation "Commission Nationale de l'Informatique et de Libertes".)

Structure

The CNIL consists of 17 members, 15 from various state organs: two members each are appointed from the following: Assemblee Nationale, Conseil economique et social, Senat, Conseil d'Etat, Cour de Comptes and Cour de Cassation; three mambers are appointed by the Cabinet, the Cabinet is represented by three members, and finally these 15 are supplemented by two people distinguished for their knowledge of data processing. All the 17 members of the CNIL are appointed for five years or the duration of their term of office. The commission chooses from among its members a president and two vice-presidents, who will also hold office for five years. Apart from normal expiration of the period of service, the term of office can either be ended only by resignation or by a decision of the CNIL itself.

To ensure the impartiality of the Commission in fulfilling its tasks, its members must not concurrently be members of the Government or employees or shareholders of a data processing undertaking. In other respects the CNIL decides on its own rules. In fulfilling its tasks, the CNIL will be supported by an administrative department, the supervision of which will be the duty of either the President of the Commission or, by delegation, one of the vice-presidents. The staff of this administrative department must be appointed by the Commission.

Tasks

The CNIL is the recipient of notifications of data pocessing in the private sector and applications for a decision in the public sector. When notifications of private data processors are received, it is obliged to acknowledge receipt thereof immediately; in the case of notifications from public data processors it must give its opinion within two months; this period can be extended for a further two months if the President of the CNIL considers such an extension desirable.

For both public and private sectors, the Commission must draw up simplified regulations for the most common forms of data processing; based on the particulars given in the standard notification, and hence contain all the relevant information connected with the data processing work.

The Commission has to set up, maintain and publish a register which contains a list of data processing systems: this register must specify:

- the law authorising the commencement of data processing, or the corresponding administrative decision and also the date of the notification;
- the type and purpose of the storage of data;
- the department where the right of access of the data subject may be exercised;
- the types of data stored and the recipients or classes of recipients who are entitled to receive such data.

In addition the CNIL must publish all its decisions, comments and recommendations, knowledge of which may be useful for the application or interpretation of the law.

Finally, it must submit an annual report to the President of the Republic and Parliament, giving an account of its activity and that of its administrative department; this report will be published.

Besides these special publication obligations, it must keep a check to ensure that the provisions of the data protection law are correctly applied; in particular it must check that the rights of data subjects are being correctly exercised, and in this capacity it is the recipient of complaints and applications or requests from both sides.

It must in addition keep itself informed regarding commercial practice in the data processing field, and adapt its decisions to the progress of science.

Powers

In carrying out its task of control, the CNIL has the following rights:

- it may by a special decision have a check carried out on the data processing equipment on the spot, and demand information and documents from the user

- it may issue specimen instructions for the security of data processing systems and order the destruction of data storage media
- it may give warnings of non-observance of data protection regulations to the users, and report to the public prosecutor punishable actions in connection with the data protection law which have come to its notice.

If sensitive data are to be stored, the CNIL can advise the Conseil d'Etat to grant a permit for this; such a permit is however justified only when public interests take precedence*.

Regarding the right of access of the data subject, the CNIL has the following rights:

- it fixes the fees for the communication of data to data subjects
- on request from the user, it may allow him time to reply to questions, and to reject obviously improper enquiries
- it may release the user from his duty to notify corrected or erased data to the recipient of such data

* This regulation does not apply to the press or audio-visual media which are permitted to store sensitive data - see above.

- requests for communication of data concerning state security, the defence of the country of public security must be addressed to it; in cases of this kind it then appoints one of its members who belongs to the Conseil d'Etat; the Cour de Comptes; or the Cour de Cassation, to make further investigations.

2.1.4 United Kingdom

2.1.4.1 Legislative Position

In the forefront of curent discussion in the United Kingdom is the Lindop Report. F1

The report does not contain a complete draft bill, but a series of recommendations. Although this involves a number of difficulties, we shall nevertheless endeavour to follow the same pattern in describing the position.

The basis of the description is the English original of the Lindop Report.

2.1.4.2 Data Protection law as a context to the Control Authority

General Preliminary Remarks

The central feature of the proposals is the establishment of a central Data Protecion Authority (referred to below by the abbrevation DPA). This prepares, for each of several specific classes of application in the public and

(Footnote 1: Home Office, Report of the Committee on Data Protection, Chairman: Sir Norman Lindop, London, December 1978, Cmdn 7341 - referred to below as the Lindop Report).

private sectors, specific regulations for data processing, which are to receive the force of law by being passed through Parliament.

Types of Data

The suggested regulations relate both to the public and also the private sector. Ptotection is to be given to personal data. "Personal data" are data which relate, or can be related to identifiable natural persons, including the data whereby they can be identified.

Types of Data Processing

The starting point is the automated processing of data, i.e. the collection, recording, assembly, storage, selection, combination, alteration, deletion, destruction, distribution, transfer, communication and publication of data, for which a device is used which can carry out stored instructions.

Conditions on which Data Processing is Permitted

Information systems are regulated by codes of practice, which are prepared by the DPA for particular types of application, and enacted by parliament. As part of these regulations provision may be made for the duty of registration.

Duties of the User and Rights of the Data Subject

Both the duties of the user and the rights of the data subject are determined in accordance with the various regulations. in this connection however a series of basic principles should be adhered to:

In the interests of the data subject:

- data subjects should know what personal data relating to them are handled, how they will be used, who will use them, for what purpose, and for how long;
- personal data should be handled only to the extent and for the purposes made known when they are obtained, or subsequently authorised;
- personal data handled should be accurate and complete, and relevant and timely for the purpose for which they are used;
- no more personal data should be handled than are necessary for the purposes made known or authorised;
- data subjects should be able to verify compliance with these principles.

In the interests of the user:

- users should be able to handle personal data in pursuit of their lawful interests or duties to the extent and for the purposes made known or authorised without undue extra loss in money or other resources.

In the interests of the community:

- the community at large should enjoy any benefits, and be protected from any prejudice, which may flow from the handling of personal data.

2.1.4.3 Control authority

For the formulation and implementation of these regulations in specific fields, a Data Protection Authority should be set up by law.

Incorporation

The DPA is to be set up as an independent and financially self-supporting institution.

Structure

The DPA should be composed of a governing board and an administrative department (executive). The Board should consist of a chairman and eight to twelve members. It would be competent for clarifying questions of principle and deciding internal questions in dispute. The Chairman or Deputy Chairman should probably serve on a full-time basis. The members of the governing Board should be appointed by the (Prime Minister) Crown and should be responsible only to Parliament, not to a minister. Only Parliament could dismiss members of the Board. Otherwise their term of office should be five years, and they should be eligible for re-appointment.

The executive should consist of approximately forty members publicly recruited by the Board. The number forty is based on a rough calculation, which as been made on the expected number of systems requiring regulation.*

All members or employees of the DPA are subject to the Oficial Secrets Act. They do not have civil service status.

* For details of this calculations, see the Lindop Report, paragraph 22.18 to 22.24.

Tasks

The tasks of the DPA are described in the Report as follows:

- The drawing up of the rules for users,
- the setting up and keeping of a register of applications for automated personal data processing (registration),
- investigation of complaints,
- supervision of compliance with the rules drawn up but above all:
- counselling of users and of affected persons.

In order to remain flexible in relation to the various forms and purposes of data processing, the DPA should be able to draw up rules (codes of practice, hereinafter described as codes) which may relate to individual users, groups of users, individual systems or groups of systems. F1

(Footnote 1: In appendix 9 to the Lindop Report, pages 409/410, 37 fields and groups of users are listed, for each of which such a code might be drawn up. These include, for example, consumer records, membership records, specified according to different types of associations, records, archives, credit card companies, empolyees' records, banks, mail order firms, address list agencies, the press, word processing systems.)

To this end the DPA should work out by a careful and gradual process the various fields of application of personal data processing, and design a structure for these by means of close discussion with the parties concerned. These codes should then be introduced into the legislative process in Parliament directly by the DPA and in this way acquire the force of law; an infringement of these rules (codes) could then be prosecuted and punished as an offence.

The codes should specify inter alia the following particulars:

- types of data,
- purpose of the data,
- types of communication and transmission,
- declarations which must be given to the data subject when collecting the data,
- measures to respect the rights of data subjects and the interests of the users,
- data security measures,
- circumstances in which the consent of the data subject must be obtained,
- nature and costs of the right to be informed.

A registration system should be linked with the codes. The whole of the national and local government sector should be subject to the duty of registration (with the exception of the national security sector). The DPA should be able to stipulate who must undergo registration

in the private sector, and when. This duty should be made dependent on whether it is useful or necessary to assist the DPA in connecion with the various codes, for example, if:

- necessary information for the preparation of the various codes can be obtained in this way,
- information regarding possible infringements against the various codes can be obtained in this way,
- specific forms of application of personal data processing can be made generally known in this way,
- it can be ensured that a certain code can be brought to the notice of the users concerned in this way.

For the forms of application liable to registration the DPA should maintain a public, generally accessible register, which should contain for instance details as to which code applies to the particular system, when this code came into force for this system, what modifications have been made for the particular user, what sanctions have been laid down against the particular user.

To prevent this register becoming a threat, it should be possible for the DPA to make exceptions to the principle of general accessibility if this is possible without any danger to the basic principles of personal data processing, and if it is in the interests of the user.

Registration shall be subject to a fee; it should be regularly renewed; the period of validity of a registration should however not be less than one year. By means of these fees, the DPA should be able to finance itself in the long term.

The duty of registration should be made publicly known or intimated directly to the user; it can come into force irrespective of a code and should then be able to be fulfilled by the more submission of a notification form and the remittance of the required fee.

The main task of the DPA towards users should however be that of advice and assistance. Users should have the opportunity, if necessary on payment of a suitable fee, to receive guidance and assistance in the planning of new and the operation of old systems. The advice given by the DPA should be binding on it so long as the system is operated in the manner made known to it, in order to avoid expensive alterations and to make possible long term planning by users. The committee, in view of the great power exercised by the DPA, paid particular attention to its answerability; the accounts of the DPA should be submitted annually to the Comptroller and Auditor General. Otherwise the DPA will be subject to the control of Parliament and the courts. The control of Parliament relates, as already described, to approval of a code and also to the dismissal of members of the Board. Public hearings held by the DPA should be subject to scrutiny by the Council on Tribunals so far as the

procedure followed by it is concerned. Finally the DPA should submit a report once a year to Parliament to make its codification policy and its practice accessible to public criticism.

Enforcement

The DPA should be in a position to carry out preliminary investigations on its own initiative. For this purpose the DPA should have the right - subject to judicial permission, which must always be obtained beforehand - to have access to and carry out searches in appropriate institutions, to examine systems and to have copies made of relevant documents.

The DPA should in addition be in a position to investigate concrete complaints. In this connection it should be able to hear witnesses and to demand documents, even from public bodies.

In the event of infringements the DPA should be able to call for sanctions from the courts: an infringement against the duty of registration should be brought before a magistrates' court.

In the case of an infringement against the codes, according to the gravity of the infringement, either the same type of court or the Crown Court would be competent. Besides imposing a penalty the court should have the right at the same time to require appropriate actions to

be taken. The DPA should however, before inititating such proceedings, carefully ascertain the facts, and discuss the matter with the persons affected. In the event of difference in interpretation, the possibility should exist of a hearing with the user concerned and/or the group with whose interests he is associated. The DPA should certainly not be entitled itself to decide regarding the guilt or innocence of the user, it should however be able to require the user to change his procedure. Its findings should be admissible as evidence in claims for damages against the user. Furthermore the DPA should then be able to initiate appropriate criminal proceedings. In an extreme case it should be possible to secure from the courts a complete prohibition of the use of his system by the user (unjunction). A data subject who has suffered ascertainable damage from the breach of a code of practice should be able to sue the user for compensation.

It would be possible to appeal to the courts - though of course only on legal grounds - against decisions of the DPA.

Finally the DPA should also be subject to investigation by the Parliamentary Commissioner for Administration (Oribudsman).

2.1.5 Ireland and Italy

In Ireland and Italy when this report was being completed there were still neither generally accessible reports by official committees nor draft laws.

2.1.6 Luxembourg

2.1.6.1 Present Legislative Position regarding Data Protection

On the 31st March 1979 the Luxembourg data protection law (loi du 31 mars 1979 reglementant l'utilisation des donnees nominatives dans les traitements informatiques - Law dated 31st March 1979 controlling the use of personal data in data processing). The Law was published on the 11th April 1979 and came into force six months later.

The following description is based on the French original published in the official Journal of the Grand-Duchy of Luxembourg, "Memorial", A - no. 29. 11th April 1979.

2.1.6.2 Data Protection Law as a Context to the Control Authority

Preliminary Remarks

The Luxembourg data protection system is a licensing system, i.e. for the operation of a data bank previous notification or application, and subsequent

authorisation, are necessary. The authority for licensing is the competent Minister for the National Data Bank Register (the Minister of Justice). He is assisted by a consultative commision (La Commission consultative) hereinafter abbreviated to Cc. The control authority is therefore the Minister of Justice, in his capacity as controller of the Data Bank Register.

Types of Data and Types of Data Processing

Protection is extended to the personal data of natural persons, corporate bodies, and associations ("groupements de fait") at all stages of data processing using data banks, including the original collection of the data.

Personal data are data referring to the persons or groups of persons named.

Data banks are collections of data which are used by computing equipment ("support informatique").

In this country also special protection is given to sensitive data, i.e. data relating to opinions or activities of a political, trade union, philosophical or religious nature, and data concerning the intimate spheres of private life. Such data must not be stored in data banks. An exception is made for membership files. The membership of a trade union may be stored at the descretion of the data subject. Such data must not be passed on to third parties.

The law applies to the public and private sectors. It applies to all data banks situated on Luxembourg territory; as regards data banks situated abroad, it relates to those using them from within Luxembourg.

Exceptions are:

- data banks which are made public by law or by decree,
- data banks which contain data which relate solely to the responsible data holder,
- data banks of international bodies such as the EEC.

Conditions on which Data Processing is Permitted.

In the private sector operation of a data bank requires permission from the competent Minister. The neccessary application of the responsible data holder for this and possibly also the actual data processor must contain:

- name, style of firm, address of the responsible data holder and the actual data processor,
- designation of data bank,
- detailed description of the purpose of the data bank,
- nature and origin of the data and their relation to the purpose of the data bank,

- in the event of communication to third parties: the nature of the data communicated and results of data processing procedures and the third parties or groups of third parties to whom the data are communicated or transmitted.

The permission is granted by the Minister after:

- a report from the Cc, or
- after expirey of a period of three months,

unless there are grounds for fearing that the facilities may be misused or an infringement against the data protection law may occur. The Minister must give reasons for his verdict; it should relate only to the data bank which is the subject of the proceedings, and should contain the period of validity (not longer than ten years). In addition the permission may contain:

- details regarding data security,
- time limits for erasing data.

Alterations require approval. The permission relates to the responsible data holder and the actual data processor, and - in the case of foreign data banks - the user; it is not transferable. in the event of infringement against the regulations, the permission may be revoked.

The decisions of the Minister may be challenged in the courts (Council of State - Legal Department) within one month.

In the public sector data banks may only be established on the basis of a law or a decree. In this connection all draft laws and decrees, giving the same details as are required in the private sector, must be submitted to the Cc for comment. In their commentary the rights of the person affected must be appropriately considered. The report may contain the same additions as the Minister's permission in the private sector. The decision of the Cc may be made by a majority vote; a minority opinion may be appended to it. The law or the decree must stipulate the period of operations; it must not exceed ten years. Data banks concerning national defence and public safety may be exempted from registration in the National Data Bank Register.

The storage and processing of data relating to criminal records (excluding bankruptcy matters) and the youth protection law are the exclusive concern of the State.

The collection and processing of medical data is the exclusive concern of medical institutions, social insurance institutions and the Ministry of Health. Details are settled by a decree with the participation of the Council of State. This settlement does not preclude date processing by third parties on behalf of the said institution.

When the permission us granted, registration in the National Data Bank Register is effected.

Duties of Users

All participants in data processing must preserve the secrecy of data.

The responsible data holder and the actual data processor must make it their business to ensure that:

- the data are kept up to data,
- correction of incorrect data is undertaken,
- out of date data or data wrongly obtained are eliminated,
- the general data security regulations established by decree with the participation of the Council of State and the Cc through the competent Minister are respected,
- the programs are designed and applied in an orderly fashion,
- the transfer of data and results of data processing is kept under supervision.

Details of alterations must be addressed to the competent Minister within a month.

Rights of Data Subjects

When data is collected the data subject must be informed regarding:

- their purpose,
- whether replying to the questions is voluntary or obligatory,
- the consequences of a refusal to answer,
- the third parties who will receive the information collected,
- the right of the data subject to be informed and to have corrections made.

This does not apply to data collection in connection with criminal proceedings.

The data subject has the right to consult the National Data Bank Register and to receive extracts on payment of the appropriate fee. The fees will be laid down by decree.

The person affected has the right to learn from the responsible data holder or th user of a foreign data bank, whether data concerning him are stored, and if so what data. This information must be given, within one month, in an objectively correct and generally comprehensible form. The fee for this information will be laid down by a legal decree. Medical data will be communicated via a doctor.

Those data are excluded from the right to be informed if they have already been communicated, or may be communicated on the basis of a law, a decree or a contract in another form than that provided. Further exceptions may be made by law or decree.

The data subject may also demand correction, completion, clarification, interpretation or deletion if the data are incorrect, incomplete, ambiguous or no longer up to data, or the collection, recording, transfer or transmission or storage of the data was impermissible. In the case of correction, the data subject has at the same time a right to reimbursement of his fee for information. In addition he has the right without expense to receive a corrected extract. Third parties who have received the data must be informed of the correction.

If the data subject has grounds to suppose that the data passed to him do not correspond to the data which have been stored, he has the right to appeal to the competent Minister, who for his part can initiate an investigation.

2.1.6.3 Control Authority

Incorporation

The functions of control are exercised by the competent Minister assisted by the Consultative Commission.

Structure

At the time when this report was being prepared there was no information available regarding the competent department of the Ministry of Justice. The Cc consists of at least five members (lawyers andd EDP experts) who are appointed by the Grand Duke for five years from suitable experts in the public and private sectors. The appointment may be renewed.

The internal procedure is controlled by decree.

Tasks of the competent Minister

The competent Minister has the following tasks, against the background of th control system:

- carrying out of the authorisation process in the private sector,
- supervision of compliance with the data protection law and its executive regulations in conjunction with the Cc,
- taking suitable measurers in accordance with the data protection law, by agreement with the Cc as appropriate,
- entry in the National Data Bank Register and delection after five years if the permission is no longer being made use of.

The National Data Bank Register contains the following details regarding each data bank:

- name, firm style, address of the responsible data holder and the actual data processor, and if necessary also of the user of a foreign data bank,
- title of the data bank,
- description of the purpose of the data bank,
- type and source of data,
- in the event of transfer of data to third parties: the nature of the data transferred andd the recipient to whom the transfer was made,
- the date of permission or the law or decree on the basis of which the data bank was established,
- the duration of the permission,
- if applicable: the date of revocation of such permission or of the dissolution of the data bank.

In an appendix the Register contains the views of the Cc on the establishment of the data banks in the public sector.

This Register is not itself subjec to the authorisation process.

The competent Minister may arrange for explanations to interested parties, as well as conveying recommendations and warnings. It is his task to supervise respect for the rights of the person affected, and it is to him that complaints should be addressed.

Tasks of the consultative Commission

The Cc prepares the reports laid down by law. It must also follow the development of data processing and advise the Government, in particular about the effects of automated data processing on the basic civil freedoms and on the functioning of democratic institutions. For this purpose it may carry out studies and investigations. It must draw the attention of the Government to unwelcome developments and gaps in the regulations. It must prepare an annual report for the Government, which will be published.

Powers of the competent Minister

The rights of intervention lie exclusively with the competent Minister. He can instruct officials to make enquiries on the spot regarding the observance of the regulations, instructions and authorisations, and gather all necessary information to this end. He reports any infringements to the competent Criminal Prosecution Authorities.

2.1.7 Netherlands

2.1.7.1 Present Legislative Position

Plans for the establishment of a central population register and the census in the years 1970/71 were the starting point of the discussion of data protection in the Netherlands. This discussion led to the setting up of the Koopmans Commission. The final report of the Commission was submitted in 1976; it contained a draft law, which formed the basis of further discussion and consideration in the Dutch Ministry of Justice. The presentation of a Government bill can be expected by the beginning of 1980.

Although it remains to be seen to what extent this draft bill will differ from the Commission's own draft, we have adopted the latter draft as the basis for the description of the Dutch position. However, irrespectivee of its actual chances of becoming law, the draft, with its emphasis on self-regulation and its simultaneous orientation towards the practice of the Swedish control authority, contains an interesting model for a scheme of control. F1

(Footnote 1: The basis of the following description is the unofficial English translation of the draft).

2.1.7.2 Data Protection Law as a Context to the Control Authority

Types of Data

The draft regulates the handling of data relating to natural persons. Some of these data - sensitive data - are subject to special regulations. Sensitive data are such as relate to religion, philosophy, race, colour of skin, political opinions, criminal or disciplinary sentences, and personal, medical or psychological data. The range of such data can be extended by decree.

Collections of data are excluded if they do not contain any other details than surname, forename, address, sex, title, profession, telephone number, and Giro account number. Data systems are also excluded which in addition contain data which simply improve the functional efficiency of the system (internal codes etc.) provided no sensitive data as defined above can be derived from these systems. Notes and correspondence of a purely personal nature and bibliographical systems are also excluded. Also excluded are non-automated systems for financial audit and book-keeping, provided that they contain no other data than that required for this purpose, and that they are communicated to third parties only as evidence for the assertion of legal claims.

By decree such data may also be excluded which must pass through another channel to identify the person concerned.

Types of Data Processing

The law covers data systems in the public and private sectors to which automated access is possible, also all systems which are so arranged that access to sensitive data is possible, as well as systems which can be used for transmitting data to third parties.

Regarding the non-automated processes the following regulations may be applied correspondingly or with appropriate modification.

In the public sector the following are excluded: Data systems in the field of public safety or security, public registers instituted by law which are generally accessible, and the State archives. Otherwise the data protection law applies if provided no variation is provided in the particular law setting up the system.

Conditions on which Data Processing is Permissible

The operation of a data bank is only possible after registration with the Registration Authority. (Hereinafter the Registration Authority will be referred to by the abbreviation RB corresponding to the English translation "Register Board"). For the registration process, three different categories are provided:

a simple registration process, a regulation process and a licensing system.

The types of procedure depends on the operator and the type of data in the system concerned.

The simple registration system covers systems which do not contain any sensitive data, and relate to membership lists, subscriber lists, salary details, debtor and creditor data, data coverning customers and suppliers, also systems of the same user in which such groups of data are linked together. This category may be extended by decree.

As part of this simple registration process the RB should be informed of the following for entry in the data register.

- Category,
- Name, address and registered office of the operator.

A charge may be made for initial registration or subsequent renewal.

The regulation process is a catch-all process for all systems which belong neithr to the category of simple registration nor to the licensing systems.

The licensing process covers systems which do not come into the sphere of simple registration, which provide for the transmission of data to third parties and/or contain sensitive data and/or in connection with which it is intended to restrict the rights to information and correction.

The granting of the licence takes place after submission of:

- the required information, as described in connection with simple registration (cf. above);
- the operating instructions (see below) and organisational measures for data security;
- any further specifications required by the RB.

The operating instructions must contain at least:

- purpose and method of use of the system,
- the category of persons regarding whom data are contained in the system,
- the type of data which is stored in respect of each person,
- the persons or categories of persons who have access to the system,
- the persons or groups of persons to whom the data will be conveyed, both inside and outside the organisation in question,
- cases in which data will be erased,
- conditions and arrangements for informing data subjects regarding the storage and the transfer of data to third parties,
- a survey of the organisation of the data system and its management.

Payment must be made for the application and subsequent renewal of the licence.

As already mentioned, the other systems are subordinate to the regulation system. This group can, like the licensing group, be specified or extended by decree. The information required by the RB is:

- the basic information
- the operating instructions.

Payment must also be made for initial application or renewal.

Alterations to the category, the operator and the operating instructions must be reported to the RB. The alteration of the category is permissible only with the consent of the RB and only subject to the necessary conditions applicable to the new category.

Decisions of the RB (e.g. refusal or registration) are subject to appeal through the courts.

Duties of th Users

The operator is responsible for observing the operating instructions; these must be kept ready for inspection by anybody, and a copy must be sent on request to anybody on payment of costs. F1

(Footnote 1: information which might endanger the security of the system, may be excepted.)

A variation from the regulations is permissible only where a law orders accordingly, or the data subject has expressly agreed thereto in writing, or where the RB agree.

The opeator of a regulated or licensed system must inform the data subject within a month of the initial storage of the information. There are however exceptions to this duty to provide information. Notification is not necessary if:

- the data subject knows or must know that the information has been stored,
- the person affected had previously been informed of the possibility of such data storage,
- or (of importance in the public sector) the system was created by law.

Exceptions to the duty of notification also exist in the case of systems which do not need, on the basis of their approved operating conditions, to provide such notification. Such exceptions may be provided for systems with scientific or statistical purposes, and for credit information systems which relate to the credit-worthiness of natural persons in their capacity as "Entrepreneurs".

The operator must, at the request of the data subject, give information regarding the data stored by him and passed on to others, and must correct, amplify, or delete data if they are not in accordance with the operating instructions or are irrelevant or incorrect.

The operator of a licensed system is moreover obliged to keep a record in an appropriate manner of the transmission of data to third parties and retain it for one year. Exceptions to this are permissible if the operating instructions already regulate such transmission in detail, and specifically if a legal decree or the RB has permitted this exception, or if the data subject receives a copy of the data conveyed.

As regards data security, special regulations may be issued by government decree, these instructions being appended to the licences or operating instructions.

Rights of the Data Subject

The rights of the data subject correspond - as far as the control and alteration rights are concerned - to the duties of the operator, to summarise:

The data subject is informed of the initial storage of his data in a regulated or licensed system, unless one of the above exceptions applies.

The data subject may obtain information from every operator regarding his operating instructions and consult the registers of the RB, or alternatively obtain copies on payment. He may demand information from operators regarding the data concerning him stored or passed on to third parties, and may demand that it be deleted, corrected or amplified.

A charge may be made for the exercise of these rights. The fees or the criteria for fixing them are laid down by a government decree.

If errors are found on examination the fee is refundable.

If an operator refuses to comply with the rights of the data subject the latter shall be entitled to address himself to the competent court or to the RB.

The data subject may be entitled to claim for compensation for injury to his feelings and also, without providing proof of who is responsible, compensation for any actual loss suffered.

2.1.7.3 Control Authority

Incorporation

The Registration Authority (RB) is an independent authority the budgetary arrangements for which are regulated by government decree.

Structure

The RB consists of a President and a maximum of two members. The President is appointed by the Crown for a maximum period of six years. Re-appointment is permissible. The other members are appointed for a period of four years and may not be re-appointed. The members of the RB select from their number the vice-president.

The RB is provided with staff to fulfil its tasks and may appoint experts to assist it further. All members and employees are bound to observe the duty of secrecy.

The internal procedure to be observed shall be defined by a legal decree.

Tasks

In the private sector the RB is responsible for dealing with application for registration, which must be dealt with within legally stipulated time limits in accordance with the conditions mentioned in the draft law. The RB has the authority to modify the various rules.

Within the scope of the law in the public sector, the RB has an advisory function in connection with systems which have been introduced by law or by decrees. The opinion of the RB must be published in the official journal. In arriving at its opinion, the RB must apply the criteria for the category under which the system would otherwise fall. Systems in the public sector which have been introduced by legal decree or law, may not be subsequently modified by the RB.

On request the RB shall assist the Minister of Justice with advice in questions of data protection.

The RB reports to the Government and to the Parliament annually regarding its activities and experiences.

The RB maintains the register already described regarding the data systems, which can be consulted by anyone free of charge.

Powers

The RB may on request or on its own initiative carry out checks, and has the necessary rights of access and inspection for this purpose, subject to the operator being guaranteed his normal legal and civil rights. The rights of access and investigation are amplified by a duty to give information and assistance to the RB.

2.2 Data Protection Control Authorities in the German Federal Republic and Sweden

This chapter provides a description of the Data Protection Control Authorities in the German Federal Republic and Sweden in context with their Data Protection Laws.

The reasons for this detailed description have already been given above, under 2.1.

The object of the description is to provide a picture of the differences between the legal provisions with which these Authorities have to cope. Furthermore a glimpse is provided of the practices of certain Control Authorities, to serve as a basis for the assessment of the function and role of these institutions (see below 2.3).

2.2.1 The Data Protection System of the German Federal Republic

2.2.1.1 The Federal Structure of the System

The German Federal Republic is a federally organised State. This results in a complex system of Control Authorities and data protection regulations.

In addition to the Federal Data Protection Law, there are the Data Protection Laws of the various Lands. F1

The Federal Data Protection Law (BDSG) applies to the public sector of the Federation and the whole private sector. The Land Data Protection Laws apply to the public sector of the particular Federal Lane involved.

The Control Authority for the public sector of the Federation is the Federal Commissioner for Data Protection (BfD), whilst the external Control Authorities for the private sector are the Supervisory Authorities (AB). It is the Federal Lands which are competent for the establishment and organisation of the AB's. The AB's are part of the Land Administration of the particular Land involved, but are responsible for enforcement of the BDSG as a Federal Law.

(Footnote 1: When this report was being completed 9 out of the 11 Federal Lands had Data Protection Laws).

The Control Authority for the public sector of the Lands is the various Control Authorities specified in the various Land data protection laws, generally a Land Commissioner for Data Protection. In this report the Hesse Data Protection Commissioner (HDSB) and its data protection law context, the Hesse Data Protection Law (HDSG) are presented as examples. F1

(Footnote 1: The Land data protection laws vary from each other however as regards the organisational incorporation of the Lane Data Protection Commissioner. These variations are however not sufficiently important for the understanding of the German data protection system to make it necessary to provide a description.)

This differential design of the data protection system - which is also difficult for German useers and data subjects to understand - required a series of coordination measures, which will be briefly discussed as they are not uninteresting in relation to the coordination problems within the EEC. F1

Uniformity of practice by the AB's is ensured by the administrative provisions of the BDSG, which were promulgated by the Lands for their respective AB's by agreement with each other. These administrative provisions contain interpretational guidelines for the application of the BDSG in the private sector.

(Footnote 1: The reasons for this differentiated system will not be discussed in detail here. They were fully discussed on the occasion of the establishment of the BDSG. In the course of this discussion other possible arrangements from the point of view of Constitutional Law were considered. In this connection we merely wish to point out that this differentiated design also makes it possible to try out various patterns of regulation and organisation. In the long term it is by no means excluded that the different arrangements will be made more uniform.)

The Data Protection Commissioners of the Lands also work together and with the Federal Data Protection Commissioner in constant consultation regarding questions of principle. Furthermore, it is one of the tasks of the BfD to ensure this general consultation, and this requirement is expressly laid down in a series of Land data protection laws as an express task of the various Land Commissioners.

2.2.1.2 Control Authorities and Federal Data Protection Law

The BDSG applies, as explained, to the Authorities and other public bodies of the Federation, as well as for the whole private sector. It constitutes the legal framework for the Control Authorities: BfD and AB.

2.2.1.2.1 Present Legislative Position

The BDSG - the full title of which is: "The Law for Protection of Personal Data against misuse in the course of Data Processing" - came into force on the 1st January 1978 with the greater part of its provisions, and became fully effective on the 1st January 1978.

2.2.1.2.2 Data Protection Law as a context for the Federal Commissioner for Data Protection and the Supervisory Authorities

Preliminary Remarks

The BDSG - as well as the Land Data Protection Laws - are subsidiary legislation. Before they are applied therefore it must be checked whether other laws and legal principles in the various fields of application do not take precedence. As regards the relationship between employer and employee for instance, the legal principles of labour law take precedence in questions of data storage and communication.

The BDSG essentially describes the substantive conditions for data processing.

Types of Data

The law provides protection of personal data, which are stored, altered, erased or transmitted in data storage media. According to the definition in the law, "personal data" means individual details regarding personal or objective circumstances of an identified or identifiable F1

(Footnote 1: For the interpretation of the expressions: "stored, alteration, erasive and communication" see the following section).

natural person: the protection extended by the Law does not cover legal persons (public or private corporate bodies).

The sphere of protection provided by the law also does not cover personal data used by press or film for journalistic purposes. F1

From the whole body of personal data two types are distinguished:

Data regarding members of an association of persons which are brought together in a list or otherwise and which relate only to:

- name,
- title, academic qualifications,
- date of birth,
- occupation, trade or business activities,
- address,
- telephone number.

Contrary to the conditions applying in the private sphere for the communication of personal data, these data may be F2

(Footnote 1: These undertakings are however not relieved of their duty to take appropriate security measures).
(Footnote 2: See in this connection the "Conditions on which Data Processing is permitted" in greater detail).

communicated if there are no grounds for assuming that such communication would infringe any interests of the data subject which are judged to require protection.

In addition, an exception is made in respect of data on health, criminal offences, breaches of regulations, religious or political opinions; different regulations apply to these (compared with other) personal data, in that they must be erased if they are found to be incorrect.

Special regulations also apply to data processed by public opinion pollsters and market research organisations; such organisations are under obligation to make the data which they store anonymous.

Personal data are protected if they are processed in data banks or communicated from such data banks. F1

Types of Data Processing

The Law distinguishes the following phases of data processing:

(Footnote 1: "Data bank" ("Datai" in German) means a collection of data organised so as to make it possible to retrieve information in different ways).

- storage: the collection, gathering or storage of data on storage media for the purpose of further use,
- communication: the making known to third parties of data which are stored or directly obtained by data processing (by the data being passed on or being held available for examination or retrieval),
- alteration: changing of the contents of stored data,
- erasure: the obliteration of the stored data.

Data processing by both automated and conventional methods is covered.

A data processor is any unit or organisation which stores data; the conception of a "storing" unit or organisation must be widely interpreted in this connection: it covers every individual authority or other public body, any natural person or corporate body, which stores personal data regarding third parties; this applies not only to the actual processing phase, but also the phases of alteration, communication and erasure. A storing unit or organisation is interpreted to include such offices or organisation as do not themselves process or store personal data, but have these activities carried out by other organisations.

Legal Conditions for Data Processing

Processing of personal data is permissible, if either:

- the BDSG or some other legal regulations permits this F1

or

- the data subject has agreed to such processing. F2

In granting permission the BDSG also distinguishes between the public and private sectors:

Conditions for the Public Sector

The storage and alteration of personal data are permissible, if they are necessary for the legal performance of the tasks falling within the competence of the public office or organisation carrying out such storage.

The communication of data in the public sector is also subject to the same reservation. An additional prior condition also applies in this case to data communicated to the transmitting office by a person (e.g. a doctor)

(Footnote 1: the term legal regulation covers all material legal rules in the widest sense, i.e. laws and decrees of the Federation and of the Lands, bye-laws and also parts of Collective Agreements).
(Footnote 2: Such agreement means previous declaration of agreement of the part of the data subject: it, must be in writing).

pledged to secrecy, or subject to a professional or official secret. The transmission of such data is permitted if the recipient requires the data for carrying out the same purposes as those for which the transmitting office recieved them.

The communication of data to the private sector is subject to the same reservation of necessity; such communication is also possible if the recipient can demonstrate a justified interest in the communication of the data, and provided that there is no infringement of the data subject's interests. If the data are the subject of a professional or official secret, it must also be checked whether the person pledged to secrecy and who has communicated the data, was entitled to do so.

Conditions for the granting of permission for Data Processing by private bodies for their own purposes

In the private sector, apart from the individual phases of data processing, a distinction is also made according to whether the data processing is for the user's own purposes or for data processing as a business on behalf of third parties.

Where the data processing is for the operator's own purposes the following applies:

Data processing by such offices or organisations is permissible provided it lies within a contractual relationship or a relationship of trust similar to that of a contract. This condition applies both for the storage and alteration as well as for the transmission of data. F1

In some cases further or less stringent conditions are imposed for storage and communication:

Storage is also permissible if it is necessary for the legitimate interests of the storing office or organisation, and there are no grounds for assuming that the ligitimate interests of the data subject are impaired thereby. If data are taken from generally accessible sources, these may be stored, but only as part of non-automated processes.

Communication is also permissible if it is necessary for the ligitimate interests of the office concerned or those of third parties or the general public. legitimate interests of the data subject must not however be impaired.

The communication of data subject to professional or official secrecy is forbidden.

(Footnote 1: Such relationships apply in the preliminary and closing stages of contractual relationships).

The communication of data in list form is permitted if no legitimate interests of the data subject are impaired.

Conditions for Permissibility of Data Processing by Private Bodies on behalf of Third Parties

Provided no impairment of the ligitimate interests of the data subject is to be feared, the storage of personal data is permissible; if the data can be obtained from generally accessible sources, their storage is permissible even without this reservation.

The communication of personal data is permissible if the recipient establishes a ligitimate interest in such communication. The justification of such an interest must be recorded. Communication of data compiled in list form (see above) is permissible if the data are restricted to the details mentioned, and there is no reason to assume that legitimate ineresting of the data subject are impaired.

Attention must be paid to ensure that legitimate interest of the person affected are not impaired by any alterations to the stored data.

Duties of Users

Besides compliance with these substantive regulations the user has the following duties:

- correction, blocking and erasure of personal data,
- notification of the data subject and the supplying of information to him,
- appointment of a Data Protection Controller, and any necessary security measures. F1

Over and above these there is in addition for all persons involved in the processing personal data, the duty of secrecy; in particular data must not be used for a purpose other than that of fulfilment of the task concerned and they must not be made accessible to unauthorised third parties. This obligation, which must be acknowledged in a formal manner, continues to apply after termination of employment.

Duties of Authorities and other Public Bodies

Data which have been proved to be incorrect must be immediately corrected; an application from the data subject is not necessary. Data must be blocked if their correctness is disputed by the data subject, or if doubts exist regarding the correctness of the data. Data must also be blocked if they are no longer necessary for the legal fulfilment of its task by the public body. Apart from storage, all other processing phases are prohibited;

(Footnote 1: "blocking means some form of access control which prevents the data being retrieved until the "block" is removed or the data erased).

blocked data may only continue to be processed for use in scientific projects, to satisfy an emergency need for evidence or to satisfy the vital interests of the storing authority, or a third party, or if the data subject has agreed.

Erasure of personal data is possible if no ligitimate interests of the data subject are impaired by such action Such erasure is obligatory if the storage itself was not permissible, or if the data is no longer necessary for the storage body and the data subject requests that the data be expunged.

Official bodies storing data must announce in the official government journal (Official Gazette) immediately after initial storage of personal data:

- type of data stored,
- purpose of the data,
- classes of data subject
- recipients of the data,
- type of data communicated.

At the request of the data subject public bodies storing data must give him information as to the data stored regarding him; they are relieved of this duty only if:

- the legitimate completion of their tasks is endangered,

- public safety and order or the public good would be prejudiced,
- the data stored must be kept secret,
- the application for information relates to whether data has been communicated to the Authorities for the Protection of the Constitution.

Public bodies are under an obligation to take the necessary technical and organisational steps for the security of the stored data. F1

(Footnote 1: As regards this obligation, administrative instructions have been published which list in detail, the steps to be taken; these administrative instructions have been drawn up in collaboration with the Lands and are therefore identical at both the Federal and Land levels).

Duties of Private Data Processers

The duties of private data processers are essentially independent of whether the data processing work is carried on for their own or for third party purposes.

Data which have been proved to be incorrect must be corrected. If there are doubts regarding the correctness of the data, and if the correctness of the data is challenged by the data subject, the data must be blocked. Blocking is also required if the data are no longer necessary; the blocking requirement in this case applies only to private data processing for the user's own purposes, whereas data processers on behalf of third parties are under obligation to review the necessity of the data on expiry of the fifth calendar year.

The duties regarding the erasure of data are however different:

- data processing for the operator's own purposes: erasure is permissible if the data are no longer required to meet the purposes of the undertaking, and there is no reason to assume that legitimate interests of the party affected will be impaired.
- DP on behalf of third parties: erasure is permissible if no reason exists for assuming that legitimate interests of the data subject will be impaired.

As soon as personal data regarding a data subject have been stored for the first time, he must be informed of such storage. The storimg units or organisations are obliged in addition to inform the data subject at his request, regarding any stored data which relates to him, if the data are subject to automatic processing, the data subject must also be informed of any recipients of the data. There is no duty to give information if:

- the business purposes and aims of the storing authority would be seriously prejudiced and legitimate interests of the data subject are not impaired by such a refusal to give the information;
- an official statement from the competent public body regarding a possible danger to public safety and order requires that the data be kept secret;
- the data must be kept secret owing to a legal regulation, or by its very nature;
- the data were available direct from generally accessible sources;
- the data has been blocked.

Private data processers employing a certain minimum number of staff must appoint a Data Protection Controller within the organisation (for details of this see the section regarding "Control Authority").

Private data processers on behalf or third parties must also give notice to the Supervising Authority on taking up their activities; this notice must specify:

- name and style of data processer,
- staff resources of the undertaking (in particular owner, board and persons entrusted with the management of DP),
- address,
- business aims and objects of the undertaking in general and of the data processing work in particular,
- type of DP equipment,
- name of Data Protection Controller,
- type of personal data stored,
- recipient(s) of the personal data.

Like public bodies, private data processers must take appropriate security measures.

Rights of the Data Subject

The person affected has the right to:

- a copy of the data stored about him,
- correction of incorrect data stored about him,
- blocking, and
- erasure of certain types about him.

Rights of the Data subject in the Public Sector

At the request of the data subject information must be given to him regarding the data stored about him. request by the data subject must as far as possible specify the type of personal data regarding which information is required. The data subject must pay a fee for the information. F1

The information may be refused if:

- the data are stored by the Authorities for the Protection of the Constitution, the Police etc.,
- the provision of the information would endanger the tasks of the storing body concerned,
- the public safety or public order would be endangered by the provision of the information,
- secrecy regulations forbid the giving of the information.

As regards the correction, blocking and erasure of personal data, the remarks under "Duties of Users" apply.

(Footnote 1: In the sphere of the Federal authorities this fee will be fixed by a decree of the Federal Government, subject to the approval of the Federal Council; it must only cover the costs directly incurred by the administrative action in question; it at present amounts to DM10.-.)

In addition to these rights, everyone has the right to consult the register maintained by the BfD regarding the automatic data storage media maintained by Public Authorities.

Finally, everyone has the right to appeal to the BfD if he believes that his rights have been infringed by personal data processing. F1

Rights of the Data Subject in the Private Sector

Everyone has the right to information regarding personal data stored which refers to him. This right is extended in the case of ADP also to the provision of information as to any third parties who have received the data.

As in the public sector the application should as far as possible specify the type of data required.

Here also the data subject may be required to pay the costs directly incurred by the provision of the information.

(Footnote 1: This right applies with regard to all Federal Authorities, etc. with the exception of the Courts, provided they have not been active in administrative matters.)

Whether or not he requests it, data subject must be informed on the initial storage of data regarding him, unless he has learned of such storage in some other way.

In certain conditions the information may be refused to the data subject; these conditions vary between the two sectors.

If the data subject requests information from private data processers handling data regarding him for their own purposes, the information may be refused if:

- the business objectives of the undertaking would be placed in appreciable danger if the data became known.
- an official statement is made of a danger to the public safety and public order through the data becoming known. This notice is given by the competent public office concerned to the storing office; this circumstance generally arises when private data processers are under contractual relationships with Authorities and concerned with matters which require secrecy,
- the data must be kept secret in accordance with a legal provision or by its essential nature,
- the data are directly available from generally accessible sources,
- the data has been blocked.

If the data subject requests information from private data processers handling data on behalf of third parties, this information may be refused if predominant interests of a third party or the public good stand in the way.

In the private sector also, the data subject has the right to complain and the right to see the data, but unlike the public sector, not to the BfD, but to the competent Supervisory Authority.

Exceptions

So far as Authorities responsible for internal and external security for the Inland Revenue and the Courts are concerned, provided they are not involved in administrative matters, a number of different special regulations apply. To some of these reference has already been made, but they will be dealt with here once more in summary fashion - especially as important restrictions of competence of the Control Authorities appear in this field.

The Authorities for the Protection of the Constitution, the Federal Intelligence Service, the Military Security Service and other Authorities under the control of the Federal Defence Minister, in so far as the security of the Federal State is affected, and the Federal Criminal Office, the Authorities of the Public Prosecutor's Office and the Police, and the Federal and Land Finance (Taxation) Authorities, in so far as they store personal

data in fulfilment of their legal tasks within the sphere of the Revenue Code for surveying and checking, are not subject to:

- the duty to publish the category of the databank ("datei") the Official Gazette,
- the duty to give the data subject information regarding the communication of data to these Offices.

A general right on the part of these organisations to refuse information applies however only if the information endangers the public safety or public order or otherwise threatens the welfare of the Federation or of a Land or if the data must be kept secret by their very nature.

These Authorities are however subject to the obligation:

- to assist the BfD in the fulfilment of his duties,
- to allow the BfD or an employee of the BfD specially authorised for the purpose the rights of access and inspection (but not if the highest relevant Federal Authority (Usually the Minister) lays it down in the individual case that this would endanger the safety of the Federation or of a Land).

The BfD will keep a special register regarding the data banks of these Authorities, with the exception of Federal Authorities or those of the Federal Office for the Protection of the Constitution, the Federal Intelligence Service and the Military Security Service.

2.2.1.2.3 Control Authorities

For the public sector of the Federation the BDSG appoints a Federal Commissioner for Data Protection (BfD), and for the private sector the Supervisory Authorities (AB) as external control authorities. In addition there are, as internal control authorities, the individual Data Protection Controllers (BDSB). The BDSB is appointed by firms which give regular employment to at least five staff in the case of ADP and twenty in the case of non-automated data processing. The BDSB must have the necessary legal and technical knowledge for this task. In the prformance of his duties he must be assisted by the undertaking. The BDSB is under the control of the legal or statutary management of the undertaking - Owner, Board of Management, Managers, etc. regarding the fulfilment of the tasks within his specialist field he has a free hand; he must not be penalised because of his duties. The individual undertaking DSB must supervise and ensure the observation of the Data Protection Reglations within his undertaking. This task involves in particular:

- the keeping of a register regarding the type of data stored, regarding the business aims and objects for the fulfilment of which the stored data are required, also regarding the recipients of the data and the nature of the automated data processing equipment used;
- the supervision of the proper use of the processing programs;
- the communication of relevant instructions and knowledge regarding Data Protection Law to the staff concerned with the processing work,
- advice in the selection of staff to be used on data processing.

Besides the authority to fulfil his tasks without detrimental consequences to himself, the BDSB has the right to appeal to the AB for checking in individual cases.

The Federal Commissioner for Data Protection (BfD)

Incorporation

The BfD authority is established under the auspices of the Federal Minister for the Interior. In addition, the necessary staff and equipment for the fulfilment of his tasks are provided by this Ministry.

Structure

The BfD is appointed by the Federal President on the suggestion of the Federal Government for a period of five years. He enters into a public legal service relationship with the Federation: he is subject to the legal supervision of the Federal Government and the service supervision ("Dienstaufsicht") Minister for the Interior; otherwise he has a free hand. As he is not a Civil Servant, his legal service position is defined uniquely by this law.

The BfD Authority has the following Departments, which also characterise the spheres of activity of the BfD:

Department I

1 Fundamental matters

1.1 Fundamental matters of data protection law

1.2 Development of general data protection law

1.3 Co-ordination of data protection in the Federal Administration

1.4 BfD's annual report.

2 Technical and organisational matters

2.1 Technical and organisational data protection measures

2.2 Inspection group

2.3 Assistance to Departments II to V in technical data processing matters and in audits

3 Keeping of the register of data banks

4 Questions of general co-operation with the Land Commissioners for Data Protection and the Supervisory Authorities of the Lands.

5 The handling of enquiries provided these do not fall within the competence of other Departments.

6 Central tasks of BfD internal adminstration.

Department II

1 General Internal Administration and branches of the foreign service of the Federal Administration.

2 Administration of justice and law

3 Finance, taxation and budget

4 Post and telecommunications

5 Data protection concerning religious bodies

6 International questions of data protection

7 Matters concerned with a number of Federal Authorities provided these do not fall within the competence of another Department.

Department III

1 Social questions, in particular:

1.1 Social Insurance

1.2 Social assistance

2 Personnel matters.

2.1 Officials

2.2 Employees, workers in the public service

2.3 Staff representation

2.4 The "Betriebsverfassung" (business constitution) law except where Department IV is competent for this

3 Public Health

3.1 Chambers and AssociatiOns

3.2 Relationship between doctor and patient

3.3 Sickness Register

4 Public relations work of the BfD

5 Matters concerning the Ministries active in the field of Social Security providede they do not come within the competence of another Departmnt.

Department IV

1 Private Businesses

1.1 Public administration with regard to commercial matters

1.2 Agriculture

1.3 Public enterprises

2 Public Transport Services

3 Education, Science and Research

3.1 School organisation

3.2 Vocational tr`ining

3.3 Science and research

3.4 Cultural institutions

4 Planning and Statistics

4.1 Planning information systems

4.2 Statistics

5 Media

5.1 Radio, Press, Film

5.2 Data protection in journalistic work

6 The non-public sector

6.1 Commerce

6.2 Professions

6.3 Parties and Associations

7 Matters of other specifically mentioned Federal Authorities, provided these do not come within the competence of another Department.

Matters of public security and defence are also dealt with.

Staffing and Budget

Apart from the BfD himself, the Control Authority had a staff of 19 in 1978, including 13 civil servants; for 1979 an establisment of 26 employees (including 17 civil servants) was planned. The total budget amounted to:

1978 1,322,000 DM,

901,000 DM expenses on personnel

1979 1,934,000 DM,

1,379,000 DM expenses on personnel.

The formal qualifications of the staff were mainly in the legal field.

Tasks

As already mentioned, the BfD controls the observance of the data protection regulations in the public sector; it

has to provide the German Parliament with an annual report regarding its activities. It also has to keep a register of those automated data banks in which personal data are processed. F1

At the request of the German Parliament or the Federal Government the BfD has to prepare and submit experts' reports.

He must promote cooperation with the Authorities, other public bodies which are responsible in the Lands for the observance of the data protection laws, and also the Supervisory Authorities.

Finally he is the complaints appeal authority for any data subject who thinks that his rights have been infringed.

Powers

The BfD may make recommendations to the public bodies under his supervision for the improvement of data protection; he may advise the Federal Government, individual Federal Ministers and all public bodies on questions of data protection. He may appeal at any time to the German Federal Parliament.

(Footnote 1: The first such report was submitted on the 1st January 1979.)

In the fulfilment of his tasks, he is entitled to demand information from the public bodies on all questions concerned with data processing, and to demand access to any premises. He can only be refused this power if inspection of documents and files would endanger the security of the Federal Republic of one of the Lands.

If the BfD discovers infringements against provisions of the data protection law, he may complain to the next higher authorities or persons responsible, and ask for their comments within a time limit stipulated by him. If the infringement in question is not one of much importance, he may refrain from making a complaint.

If he complains regarding infringements, he may also at the same time put forward suggestions for rectifying the faults.

The BfD keeps a register of automated data banks, in which personal data are stored. The register can be examined by anyone. (For exceptiions please see above). For the purpose of the preparation of the register, the Authorities report their data banks, and they may also give at the same time the following details. F1

(Footnote 1: These are laid down by the Data Protection Register Regulation dated 9 February,1978, Article 2):

1 Designation of organisation concerned

2 Category of data subject

3 Types of personal data stored

4 Tasks for the accomplishment of which knowledge of the data is require,

5 Offices or organisations to which the personal data are regularly communications,

6 Types of data to be communicated and the purpose for the communication in each case, subdivided according to the offices and organisations mentioned under 5.

Inspection Procedure

A number of inspections have already been carried out by the BfD so that it is possible to get an initial view regarding present practice. F1

For each investigation the expenditure of about 20 man days is estimated (10 man days for preparation and subsequent evaluation; 10 man days with 2 employees on the spot). This estimate is considered to be on the small side for large users.

(Footnote 1: The following description is derived from Lutterbeck, B. "Erfahrungen" - Experiences - see 2.6 - Bibliography).

The investigations have so far to be limited to spot checks. The criteria for selection were principally:

- sensitivity of the data,
- technical development stage,
- importance of the institution in question,
- applicability of the results to other institutions,
- explicit complaints.

The inspection begins with a conversation with the managers and employees responsible for data protection. With the help of the internal data catalogue the inspectors get a general idea of the internal structural and procedural organisation. This is of primary importance because there seems to be a close connection between conflicts within the organisation and the probability of infringements against data protection.

The next day is usually devoted to the technical organisation of data processing with its consistuent elements:

- computer centre (operation and organisation),
- software development (organisation and supervision),
- program documentation (comprehensibility).

On the basis of these investigations other investigations are then made in the specialist department. Then further discussions take place with the staff, in order to explore alternatives. This is also the main purpose of such inspections: weak points are discovered jointly with the user and possible solutions developed. At the end of the inspection the concluding discussions with the Management take place, in which the results of the investigation are discussed. The outcome of the discussions is then confirmed in a letter to the organisation.

The Supervisory Authorities (AB)

Incorporation and Structure

Supervisory Authorities are the competent authorities in accordance with the law of the "Land"; their staffing and the provision of finance is in accordance with Land Law. Among the Lands, the data protection laws of Hesse will receive a more detailed description than the others. In Hesse the Government Presidia Darmstadt and Kassel are authoritative. In the Kassel district the work is done by a "Referent"* (a higher grade civil servant) and a specialist assistance. In the Darmstadt area it is done by a "Referent" on a half-time basis (who also carries out certain trade-supervision functions).

Tasks

On request the AB carries out investigations of any data processing bureaux in the private sector which process personal data for their own purposes and have their premises within the territory of the particular AB in question. The requested investigation is put in hand:

- by a reasoned complaint from a data subject,
- in response to a request for help from a BDSB.

In the sphere of data processing by private bodies, which process data as a business on behalf of third parties, the Supervisory Authorities must keep a general watch on the activities of such bodies and also keep a register of them. In this connection the particular undertaking has to be reported, as well as branch offices and non-independent subsidiary establishments. The application must contain:

1 name or style of the undertaking,
2 responsible managers of the undertaking and the managers of the data processing department,
3 addresses,
4 business aims and objects of the undertaking and of the data processing work,
5 type of automated data processing equipment used,
6 name of BDSB,
7 type of personal data stored,
8 when personal data are regularly communicated: the recipient and nature of the data communicated.

The AB plans its inspections on a rotation system based on the register.

Powers

In the performance of its duties the AB has the power;

- to require information from the private organisations,

- to enter premises and business offices for the purpose of inspection,
- to inspect business documents.

The AB may call on the assistance of the BDSB in carrying out an inspection, but it has no power to demand the elimination of a fault. It can only refer the data subject to his legal rights, or report any important faults to the competent authority, in accordance with the "Business Code" (Gewerbeordnung), or else institute legal proceedings for breaches of regulations.

2.2.1.3 Control Authority for the Hesse Land Data Protection Law (HDSG).

First the specific legal background will be described.

As has already been made clear, what is involved here is data processing in the public sector of the Land. The Data Protection Authority for Hesse and its legal background require special attention for a number of reasons:

The Hesse Data Protection Commissioner's Office (HDSB) has been in existence since 8 June 1971. The Authority is the oldest of its kind. It has an extensive background of experience which has been referred to repeatedly in connection with the establishment of other authorities and which has thus had a substantial influence on international development.

Quite early on, the Hesse Authority developed a series of instruments and succeeded in achieving a high standard of acceptance by those for whom it operated, which set the trend for the role for data protection control authorities in modern industrial societies, and which make it clear how valuable a position these authorities occupy in the development of data processing policy and data processing law throughout the world.

Owing to the predominant historical significance of the Hesse Authority, it has also had a particular influence on international developments. As a result this Authority now has numerous contacts abroad.

To understand developments in Germany, the cooperation between Federal data protection and Land data protection and Supervisory Authority must be understood. It is therefore necessary to go into details of the Land data protection authorities, and for the reasons described it seemed most advisable to choose the Hesse Data Protection Commissioner as the Authority of greatest significance.

2.2.1.3.1 The Present Legislative Position

The first Hesse Data Protection Law came into force in 1971. As a result of the BDSG, the HDSG was amended and came into effect in its new form with the expansion of the provisions for data security, on the 1 January 1978. The data security regulations came into force on year later. The basis of this description is the original German text.

2.2.1.3.2 The Data Protection Law as a context to the Control Authority

Types of Data

Protection is extended to personal data in the public sector. Data are deemed to be personal if they contain details regarding personal and objective circumstances of an identified or identifiable individual.

Types of Data Processing

Protection is extended to data round in data banks ("datei"), irrespective of the particular process used. However, the regulations for data security also apply to non-automated processes even when data are not passed on to third parties.

Field of Application

The Hesse data protection law applies to data processing in the public sector in the Land of Hesse (see above).

The following are exempt or subject to modified regulations:

- businesses incorporated under public law of the Land: these are subject to the provisions of the Federal Data Protection law for similar undertakings in the private sector;

- credit and insurance undertakings of the Land incorporated under public law are subject on the one hand to the provisions of the BDSG for the private sector (but not, like the above-mentioned undertakings, to the supervision of the HDSB, but carry out internal checks by means of an internal data protection controller, and are otherwise subject to the control of the relevant AB.

Personnel data relating to employees of public bodies is subject to the relevant law for the private rather than the public sector, but it is supervised by the Land Commissioner.

Conditions on which Data Processing is Permitted

The implementation of data processing systems in the public sector does not require any special permission from the point of view of data protection law. However, the implementation of a new system passes through several checking processes for reasons of co-ordination and economic efficiency, in suitable co-ordination committees, in which attention is also paid to the views of the HDSB.

Duties of Users

The duties of users of data banks in the public sector of the Land of Hesse are similar to those of the Federation with the following variations:

The provisions regarding communication also apply between parts of a public administration organisation which look after different tasks or which are in separate premises. The recipient in the private sector of data from the public sector is also under obligation to use the data only for the purpose for which the public sector received the data. The publication obligations of the public operator of the Land in the Official Gazette are regulated by a special legal decree. In addition the measures for the carrying out of the HDSG are listed in a special Order (Order of the Hesse Minister of the Interior II A 4-3d 10-15 of 2.10.1978), with a recommendation to the minicipalities and other communal organisations to follow a similar procedure. Details of the measures applicable to each authority are as follows: F1

- appointment of an official for data protection questions,
- the preparation of a list of data banks to which the data protection law applies,
- investigation of data processing previously carried out and the institution of appropriate alterations,
- instruction of employees and their commitment to data secrecy,

(Footnote 1: see the Order quoted)

- organisation of the right to information and duties of notification, the latter only in the case of business in the public sector (of the Land),
- organisation of publication,
- organisation of requests for alterations by data subjects,
- notification for the data bank register of the HDSB,
- obligation of persons engaged (service undertakings),
- measures for data security.

In the list, which also serves as an internal summary, as the basis for publication in the Official Gazette, and as the basis for the data bank register of the HDSB, the following details must be given:

- details of the data storing office or organisation,
- details regarding the data bank (type of processing, whether in accordance with the operator's own process or the standard process for the Land, registration number of the process, computer centre), classes of data subject included,
- tasks for the fulfilment of which knowledge of the data is required, and the legal basis of the data compilation,
- offices or organisations to which personal data are regularly communicated,
- types of the data to be communicated,

- tasks for the fulfilment of which communication is necessary and the legal basis on which communication is carried out,
- offices or organisations entrusted with the compilation or further processing of the data, including the type of processing.

This data bank catalogue services for three types of data collections or publications. F1

- as an internal summary (Article 5 sub-section 1 HDSG); this contains all the data listed;
- publication in the appropriate Official Gazette (Article 17, section 1 HDSG);
  it contains the type of the personal data stored by then or on their behalf, why the data is necessary, the classes of data subject included, the offices or organisations to which personal data are regularly communicated, and also the type of data to be communicated,
- the HDSB data bank register (Article 25 HDSG): which also contains all this data.

Rights of the Data Subject

The rights of the data subject are as described in the BDSG. He has the right in certain circumstances:

(Footnote 1: the same publication obligations are imposed by the BDSG):

- to be informed,
- to have corrections made,
- to blocking or erasure of data relating to him,

and also the right to appeal to the Land Data Protection Commissioner.

In Hesse the data subject has also, a right to compensation "on strict liability" (ie without proff of negligence or malice).

Special Regulations

The HDSG has paid special attention to the problem of distribution of information between the Parliament and the Executive. Thus the HDSG mentions as a goal of the data protection law, not only the protection of the citizen, but also the guarangee of the constitutional structure of the State, based on the principle of the division of powers, in particular the constitutional organs of the "Land" and the organs of local self-government in relation to each other, as requiring to be protected against change as a result of automated data processing. (Article 1, Para. 2 HDSG).

This task has found expression firstly in the specific tasks and in the incorporation of the HDSB (see below 2.2.1.3.3). Secondly, there is provision in the HDSG for a special right of information enjoyed by the Land Parliament and the local representative bodies.

Finally, special consideration has been given to the interests of scientific research. For example, Article 15 HDSG lays it down that research institutions established by public law for the purpose of research may store and alter personal data, and that data from the public sector may be communicated to them for this purpose. It is of course a pre-condition that the data subjects must have agreed to this or that their legitimate interests shall not be impaired owing to the nature of the data, owing to their public availability, or owing to the nature of their intended use. Further communication is only possible with the agreement of the data subject.

2.2.1.3.3 Control Authority

Incorporation

The Authority of the Land Data Protection Commissioner is independent. As such an independent body its budget is specially ear-marked in the budget of the Land Parliament. The HDSB is appointed by the Land Parliament on the recommendation of the Land Government and is independent and free from instructions or terms of reference. He is also not subject to any legal supervision of his service.

Structure

The Authority of the HDSB has at present, in addition to the Commissioner himself, four higher grade civil servants, and contracts for the services of an outside expert. Owing to the small number involved and the wish to incur as little organisational expense as possible, particular importance is attached to constant co-operation between the members.

There are four Departments:

- Applications of data processing,
- Security sphere,
- Health and social administration sector,
- Sector for cultural administration, planning, distribution of information and inter-departmental co-ordination.

Qualifications

As regards formal qualifications, the members are described as:

- 1 person with administrative experience.
- 3 people with a legal background, one of whom is also a sociologist.

It should also be emphasised here that the qualifications must include knowledge of data processing and organisation. Furthermore the HDSB has a right to be consulted on the selection of his colleagues; the employees are subject to his instructions alone.

Tasks

The HDSB has the following tasks:

- He keeps a watch on compliance with the Data Protection Law and other data protection regulations.
- He watches the effects of automated data processing on the method of working and competence in decision making of the Land Administration.
- He pays attention to the question of whether there is a threat to the principle of the division of power from uneven information distribution, the structe of the State, and must suggest compensatory measures.
- He co-operates with the other Control Authorities of the Federation and the Lands, as well as with the Supervisory Authorities.
- He acts as adviser to the Land Government and the Authorities in data protection questions.
- He issues reports and carries out investigations on behalf of the Land Parliament and the Land Government.

- He submits an annual report regarding his activities to the Land Government and the Land Parliament. The Land Government submits its comments on this report to the Land Parliament.
- He maintains a register of data banks.

The register contains a list of all data banks to which the HDSG applies. All public data processing offices and organisations of the Land of Hesse must notify their data banks for inclusion in this register. (There is in addition the obligation to publish the data banks in the Official Gazette intended for the purpose - see above). This does not apply to Authorities responsible for the protection of the Constitution. For the remaining security authorities and the Land financial or taxation aurthorities (in so far as they receive personal data in course of their tasks for supersion and checking), a special register is kept. The rest of the register is publicly accessible.

It is planned to use a computer for keeping the register, and this should be completed by the beginning of 1980. In this connection, special attention is being paid to the achievement of extracts intelligble to data subjects, with the object of increasing the general understanding of data processing in public administration.

Powers

For carrying out his tasks, the HDSB has a right of access and inspection which is subject to limitations corresponding to those of the BfD. The HDSB also have a right of control of private bodies when they operate on behalf of public offices or organisations of the Land.

If the HDSB discovers defects or infringements, he sends a complaint regarding these to the appropriate administrative organs and demands their reply within a time limit set by him. This reply must contain a description of the measures which have been taken to put the matter right. If the faults are of no great significance, these steps need not be taken. The HDSB may accompany his complaint with proposals for remedying the matter.

With about 4000 public data storing bodies under his supervision, the HDSB can only carry out his inspection activity on a random basis, or in the light of explicit requests by data subjects. This makes the development of his preventive functions all the more important. It is particularly desirable that he should be called in well beforehand when computerisation is being planned, and also when the Federal or Land Authorities are planning legislation which may affect institutions under his jurisdiction.

2.2.2 The Swedish Data Protection Authority and it context of Data Protection Law

2.2.2.1 Present Legislative Position

The Swedish Data Law ("datalagen") became law on the 11th May 1973. It was therefore the first State data protection law (after that for Hesse, which was of course a Land data protection law). A part of the law came into force on the 1st July 1973; but it has been fully in force since the 1st July 1974.

The general development in the field of data processing, developments in the small computer market and word processing, the practice of the data protection control authority and the results of the DALK Investigation led F1
to an alteration in 1979 (minor alterations had already been made before) of the data law by means of a revised law (1979:334), which specified a number of criteria for the method of procedure of the control authority and permitted a number of simplifications.

The basis of the description is the English translation commissioned by the Dateninspektion (hereinafter referred to in accordance with the English translation "Data Inspection Board" by the abbreviation DIB) in its form dated 1st July 1979.

(Footnote 1: Delbetankande av Datalag - stiftningskommitten, 1978).

2.2.2.2 Data Protection Law as a context to the Control Authority

Preliminary Remarks

The Swedish data protection system is a licensing system. The Data Law prescribes only in general how data banks containing personal data must be conducted, and appoints the DIB as a licensing and supervisory authority to publish specific regulations for data banks.

Types of Data

Protection is extended to data which relate to natural persons, provided such data are kept in automated files in lists or in some other way, and subject to the data storage being effected with the assistance of automated data processing.

The Data Law relates both to the public and private sectors.

Special protection is extended to data relating to:

- punishable offences,
- measures in accordance with the Child Welfare Act,
- alcoholism,
- psychiatric measures,
- measures in accordancew with the Law for the Prevention of Public Dangers through Unsocial Behaviour,
- measures in accordance with the Aliens Law.

Such data banks may be compiled only in the public sector and only in accordance with a legal instruction, and then only for special reasons.

Data relating to:

- the health of a person,
- persons who have received social assistance payments,
- persons who have undergone treatment on grounds of liability to disease,

may only be processed in the public sector and only if there are special reasons for so doing.

Data relating to the political or religious convictions of persons may be stored only if there are special reasons for so doing; the organisations may undertake the automatic processing of data banks of their own members.

Types of Data Processing

As already mentioned, the processing of personal data by means of automated data processing comes under the protection of the Data Law.

Exceptions to this are automated data banks which, owing to their technical equipment, the installation, and the process used, obviouslhy do not involve any risk for the data subject. Modifications of these regulations may be made by the Government or the DIB.

Conditions on which Data Processing is permitted

The setting up of a data bank in the private sector is permissible only if the DIB has given a permit for this containing in detail the instructions for the operation of this data bank (see below 2.2.2.3). The setting up of a data bank includes the stage of compiling the data for a data bank.

Trivial forms of automatic data processing are excluded (see above "Types of Data Processing') but even such data banks may be included by the DIB if it is found that they involve a risk.

Data banks which contain information about persons other than member, employees, customers, or persons standing in a similar relationship to the person or organisation responsible for the data bank may be set up only if there are special reasons for doing so. These data banks are then in practice subject to the full licensing process (see the more detailed comments below at 2.2.2.3), whilst for the first mentioned data to be processed a simplified procedure is laid down.

The licensing system generally applies also to the public sector, with the exception only of those data banks which are set up on the basis of a legal instruction. In this connection the DIB must be consulted before the working instructions for this data bank are laid down in this

instruction. In practice there is such close co-operation here that the regulations for the data bank can only be regarded as issued by the DIB. (Examples for such co-operation are the Land Register and the Police Register.) The right of access to the data banks in the public sector may be restricted (see below "Rights of the data subject").

Duties of Users

The user must generally make sure that no harm is done to the data subject by the handling of personal data. Against this background, the DIB checks the particulars of the data bank and issues appropriate regulations for it together with a licence. The operator may however accept a set of DIB regulations previously issued for other data banks, and align his data bank with these from the outset, in order to simplify the procedure. In this connection, please see the details in the description of the procedure at 2.2.2.3 below. Furthermore, the rights of the data subject are laid down in the Data Law as obligations for the operator.

Rights of the Data Subject

With the exception of trivial data records, the data subject has the fundamental right to be informed by the responsible data keeper of the data stored about him.

The information is generally free of charge, but the DIB may allow fees for certain data records. A request for information must be complied with once per annum only. The information may - with the approval of the DIB - be refused if no risk is involved to the privacy of the data subject. This right to be informed does not apply to data which must not be communicated because of a legal instruction or a decision of the administration based upon such a legal instruction.

If the data subject requests it, he must be informed when data about him are erased or corrected.

The data subject also has a right to have the confidentiality of his data respected by all persons concerned with the data processing. This also applies to the recipienta of data who have received them on these conditions. The duty of confidentiality also applies to all members of staff of the DIB.

2.2.2.3 Control Authority

General Structure

The activities of the DIB are managed by a Board and carried out by the Administration Department.

Functions

The main functions of the DIB are:

- carrying out the licensing procedure,
- development of general guidelines for the operation of data banks as part of the licensing procedure,
- co-operation in the implementation of data banks in the public sector,
- control of the implementation of the Data Law.

Besides data protection, the DIB also carried out functions in accordance with the Credit Information Act and the Debt Collection Act.

Powers to Issue Regulations

When granting a licence, the DIB must consider both the type and the nature of the stored data and also the possible effects on the data subject. In particular the following criteria must be assessed:

- the scope and nature of the stored data,
- the manner in which the data are collected and from whom they were collected,
- the attitude of the data subject to the question of storage,
- the need for collection and processing of the data.

The licence is provided together with guidelines regarding the purpose of the data bank, the nature of the information required, and the duration of the data bank may be prescribed.

Further limitations may be laid down if there is a risk of interference with the privacy or the reputstion of data subjects. Such measures must especially be considered if the information stored consists of judgements or assessments of the data subjects.

Such limitations may also be imposed regarding the data banks in the public sector, unless such regulations are already contained in the legal provisions authorising the data bank.

In the public sector, the DIB must however make sure that the constitutional principle of free access to administrative information is not impaired.

In detail the DIB regulations may contain provisions regarding:

- data collection,
- the process of automated data processing,
- technical equipment,
- the manner in which personal data are processed,
- information to data subjects,

- the types of data which are made accessible,
- any communication and subsequent use of the data,
- the method of storage and the methods of ensuring that the data are kept up to date,
- the supervision of the data processing and data security.

Powers of Supervision of the DIB

The DIB supervises the operation of the data bank and compliance with the specific regulations in force. It must make sure that no infringement of the privacy and the personal reputation of the data subject takes place. This supervision must however be so exercised that it does not lead to any heavier costs or interference with activities than are absolutely necessary. In its execution of these tasks it has the following powers:

It has a right of access to the computer centres, the computers and the computer files.

It may demand from the responsible data keeper all relevant information regarding the operation of the data bank.

If the rights of the data subject are infringed, or if there is a threat of such infringement, the DIB may issue additional regulations.

Measures of Compulsion

The DIB may impose fines if the responsible data keeper refuses the DIB the required access, or does not fulfil his duties regarding the quality of the data and the rights of the data subjects.

If these measures do not suffice, the DIB may revoke the licence and forbid further data processing.

Advisory Functions of the DIB

One of the most important tasks of the DIB is however that of giving advice. The DIB is usually involved at the planning stage, of the setting up of complex information systems and also on the introduction of new information technologies. In this way the user saves himself from subsequent modifications of his system to meet the requirements of data protection and data security. Apart from this counselling practice, closely linked to that of licensing, the staff of the DIB are involved, by their being invited to sit on various committees or boards, in the whole development in the information processing sector, including its social effects and its influence on information processing policy.

Besides this, the experience and decisions of the DIB represent a valuable source of information for scientists concerned with social developments of data processing.

The DIB strongly sypports this research and itself profits from the results.

Organisational Structure

The DIB comprises the Board and the Administrative Department, which is split up into various sub-departments and sections.

FIG. 2.2.2.3 - 1

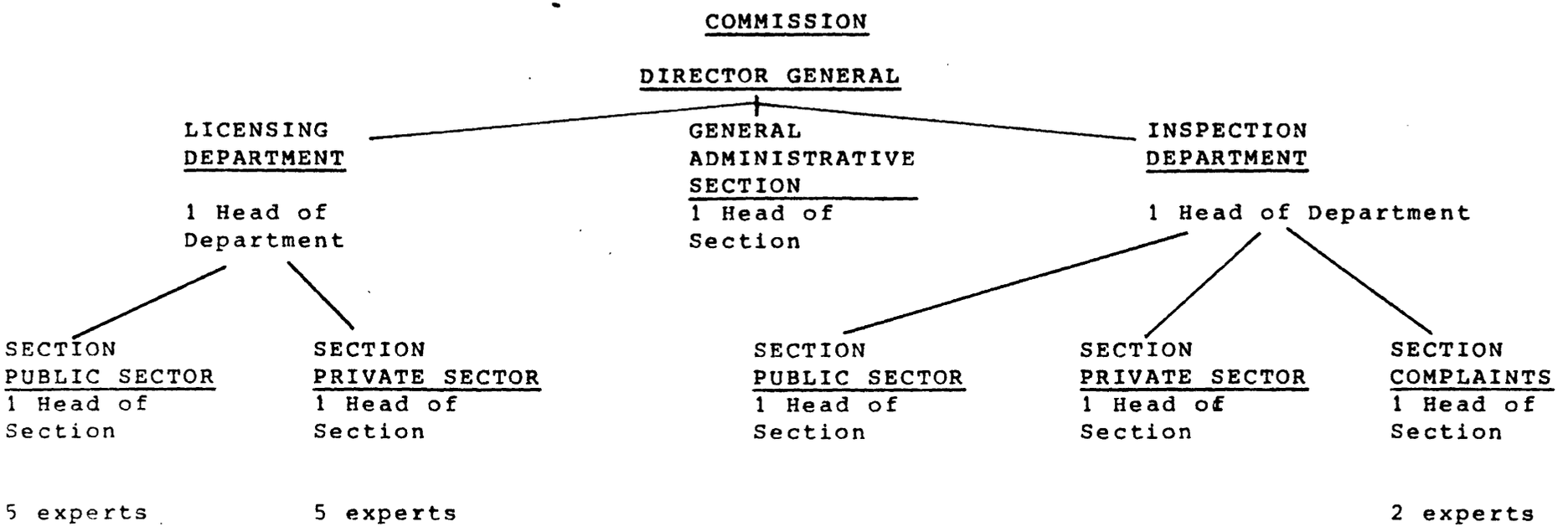
The Board

The Board supervises the activities of the Administration Department and makes decisions on matters of principle.

The Board consists of 11 persons:

- the Director
- (he is appointed for life and must have experience as a Judge),
- four representatives of the political parties,
- one representative each of the blue collar trade unions and the white collar unions,
- one representative of Swedish industry,
- one representative with experience in public administration,
- one representative with experience in computer science,
- one representative of the medical profession.

FIG. 2.2.2.3 = 1


COMMISSION
DIRECTOR GENERAL
LICENSING DEPARTMENT
1 Head of Department
GENERAL ADMINISTRATIVE SECTION
1 Head of Section
INSPECTION DEPARTMENT
1 Head of Department
SECTION PUBLIC SECTOR
1 Head of Section
5 experts
SECTION PRIVATE SECTOR
1 Head of Section
5 experts
SECTION PUBLIC SECTOR
1 Head of Section
SECTION PRIVATE SECTOR
1 Head of Section
SECTION COMPLAINTS
1 Head of Section
2 experts

The members of the Board (except the Director) are appointed for four years by agreement with the various organisations of the Government.

In addition there are seven deputy members of the Board who may represent any one of these ten Board members. The Board at present meets about ten times per annum. During these meetings, the appropriate competent members of the staff of the Administrative Department are usually present, in order to report on developments and to take part in the discussion.

The Administration Department

The Administration Department consists of two sub-departments, the Licensing Department and the Inspection Department. The first is divided into two sections, one responsible for the public sector and the other for the private sector. The Inspection Department consists of a section for complaints, and two sections for carrying out inspections in the public and private sectors respectively. The last section is to be extended, especially as three of its members are also concerned with the application of the Debt Collection Act. Since most data banks have now been licensed and registered, more attention can now be devoted to the inspection procedure.

Like the Director, his deputy in the Administration Department is appointed by the Government for an unlimited period.

Staff

The Administration Department consists of about thirty employees, excluding the Director. Nineteen of them are experts, the others are administrative staff, who are however given special training to enable them to fulfil some specialist tasks relating to data protection.

Qualifications

The majority of the higher administrative officials have a legal education, five have an education in computer science, and another two of these have a formal double qualification. The employees with legal qualifications also have basic knowledge and experience in the field of computer technology.

The Licensing Process

The Simplified Procedure

When applying for a licence for his data processing system, the user finds from a handbook issued by the DIB the appropriate category under which his system falls - for example:

- customers' and suppliers' data banks (not banks and insurance companies),
- data banks of tenants,

- employee data banks including payroll data banks,
- subscribers' data banks.

The handbook contains detailed instructions must be satisfied by the system in one of these categories. Thus, for instance, customers' and suppliers' data banks may only contain details of name, address, telephone number, delivery instructiions, registration number of firm, category, customer's number, account number, personal identity number and Giro or other bank account numbers. These details may only be recorded with the agreement of the data subjct or on the basis of a legal instruction (e.g. address alteration service of the communal authorities). Further data may only be contained if they have been compiled for data processing by the responsible data bank keeper for his own purposes, and are within the scope of the purpose for which the data bank was compiled. Data may only be passed on to other quarters with the agreement of the data subject, or in compliance with an instruction from a court or Parliament or a legal instruction or collective agreement (between employers and employed). The data banks must be accessible for correction and updating. Storage and backup must be secure. The data processing procedures must be documented.

If the user wishes to adhere to these or similarly detailed instructions for the category concerned, he requests that a suitable application form should be sent to him in which he generally only need specify, apart

from the basic particulars about his person and the technical system, the category of data bank, and declare that he will follow the instructions of the DIB for that category. His application then receives from the Licensing Department a registration number and is stored in the data bank register of the DIB. If the DIB official concerned considers that the conditions for the simplified process apply, he sends the licence, after invoicing the fee, along with the appropriate instructions by c.o.d. to the applicant. On payment of the fee the applicant receives the licence and may begin data processing.

If the applicant intends to deviate from the instructions of the DIB, or if the DIB doubts whether the comditions of the simplified procedure apply, the standard licensing procedure should be adhered to.

The standard Licensing Process

In this case the operator submits an application which must contain the following details:

- name, address, telephone number of the responsible data keeper,
- title of the collection of data in question,
- the purpose of the data compilation,

- a list of the types of data which are to be incorporated in the collection, including sources and the organisations to whom data are to be communicated, also the type of data processing,
- data handling procedure,
- rights of access to the data and types of availability,
- a description of the technical equipment and procedures,
- the way in which the rights of the data subject are to be satisfied, and whether any charges are to be made for this,
- how and when correction procedures for incorrect data are to be carried out,
- how the security of the data is to be ensured and when and under what conditions data are to be erased,
- what data security measures are to be adopted.

In this case also the applicant receives a registration number. According to the degree of difficulty involved the granting of the licence will then be discussed either at section or departmental level, or if questions of principle are involved by the Board, and suitable regulations drawn up. In this connection it is also possible that the applicant will recieve a temporary licence, so that the effects of the system can be kept under observation.

The remaining procedure then continues as in the simplified procedure. The granting of the licence will then be entered in the register with its specification.

The same procedure applies to applications for alterations.

Approximately 75% of all applications follow the simplified procedure so that here we can actually speak of a de-facto registration procedure. But even for the remaining processes, the aim is to carry out the licensing procedure in as non-bureacratic a manner as possible.

An open door policy, constant contact with applicants and constant discussion among the staff, and the use of the modern technologies of automated data recording and use of electronic word-processing make their contribution. Because of this atmosphere of constant discussion and mutual education of the staff, and also from the increased experience of the DIB in general, it has proved possible to progressively delegate decision-making to lower levels within the DIB, (see fig 2.2.2.3-2).

FIG 2.2.2.3 - 2 (LEVEL OF DECISION-MAKING)

FIG. 2.2.2.3 - 2

	FIRST YEAR	1978
COMMISSION	15%	5 %
DIRECTOR GENERAL	25%	5 %
HEAD OF DEPARTMENT	60%	30 %
HEAD OF SECTION	only since 1977	60 %

Charges

The charges for the licensing procedure are calculated on the basis of estimated working time. The details are laid down in a suitable tariff. In the case of difficult systems a special price may be fixed. The DIB's income, which at present amounts to about Swedish Kroner 1,000.000 in the budget year, goes to the ministry of Finance.

Inspection Procedure

The inspection department is able presently to carry out about 50-60 inspections a year.

Inspections are carried out partly in accordance with a predetermined plan, and partly on the basis of a complaint. Such an inspection plan may for example, have the objective of investigating service bureaux. When investigating service bureaux it is possible that users will be discovered who have not got a licence. Planned checks are also made on systems which have been granted a temporary licence.

The ckecks are not carried out only by officials of the DIB and, indeed, outside experts can be brought in for special problems.

The normal investigation team consists of a data-processing expert and a legal expert. Inspection starts with a perusal of the data about the undertaking which is stored at the DIB. From this, a few crucial points can be found on which the investigation group can then concentrate.

The responsible data keeper is usually informed in advance of the inspection so that the appropriate staff can be available to the inspection team. Only about two inspections a year are made without advance warning. The notification is genreally accompanied by a check list, with the aid of which the inspection can be prepareed for by the staff of the responsible data keeper.

The actual inspection usually starts with a tour of the undertaking during which the physical security arrangements are checked. At this stage the inspection group obtains, by visual inspection and by an interview with the responsible person, an impression of the organisation and the data processing arrangements, which shows whether and to what extent the responsible keeper has understood the problems of data protection (as an organisation problem also) and data security, including the organisational implications.

After this the documentation of the system, the data stores and individual processing procedures are checked. A normal inspection lasts half to one day. The DIB draws up a report on the inspections showing faults and

suggested remedies and sends it to the responsible data keeper in order to give him the opportunity to take corrective action, or to object. If no agreement can be reached the DIB then takes the compulsory measures at its disposal.

Although these inspections generally procede without compulsion, they do, however, not lack the necessary intensity. The main policy of the DIB remains, however, to introduce good practice rather than to apply sanctions.

With the growing experience of the DIB, the staff of the inspection section are often asked for advice on data security measures in order to avoid offences.

Technical set-up

In order to carry out the inevitable clerical work, the DIB uses an automated word-processing system which, at relatively low cost, enables decisions, licences and special provisions to be generated by extraction from a set of pre-written text modules. The register is kept by a service bureau whose services recently cost the DIB approx. 250,000 Skr per year.

For reasons of economy, but also on principle, the DIB is planning to operate its own computer centre.

Budget

The budget of the DIB is part of that of the Ministry of Justice, under its own heading. For the year 1980/81 5 million Skr is budgeted. The development of the budget is shown in the following table:

TAB. 2.2.2.3 - 1 DEVELOPMENT OF THE BUDGET

The previous activities can be seen from the following table, where:

A Total of the yearly activities

O Unfinished matters at the end of the year

The code numbers have the following meaning:

Licensing Procedure

11 Provisional licences

12 Licences in normal procedure

121 Licences in simplified procedure

13 Registrations in the public sector

14 Amendments

15 Licences in accordance with the Credit Information Act

16 Manual credit information systems

17 Automated debt collection procedure

18 Manual debt collection procedure

19 Miscellaneous decisions

The budget year runs from July to August
Figures : thousands of DM

	voted budget 77/78	real exp. 77/78	voted budget 78/79	proposed budget 79/80
EXPENDITURE				
Authorisation	875,7	1359,45	935,1	1260
Inspection	900,9	688,5	1143	903,15
Information and internal administration	82,8	3,6	82,8	82,8
TOTAL	1859,4	2051,55	2160,9	2245,95

Inspection Procedure

21 Complaints (Data Act)

22 Complaints (Credit Information Act)

23 Complaints (Debt Collection Act)

24 Initiatives of the DIB (Data Act)

25 Initiatives of the DIB (Credit Information Act)

26 Initiatives of the DIB (Debt Collection Act)

28 Inspections

29 Miscellaneous decisions

Internal Administration

71 Decisions regarding budget

72 Decisions regarding personnel matters

79 Other administrative decisions

81 Comments, general

82 Comments on complaints

91 Miscellaneous comments

TAB. 2.2.2.3 - 2 ACTIVITIES OF THE DIB

Responsibility of the DIB

Appeals against the decisions of the DIB can be logded with the Ministry of Justice by an applicant or the data subject. The Attorney General can lodge appeals in the public interest. F1

(Footnote 1: Up to now there have been about 50 appeals, the majority of which were against the amount of the licence fee).

2-171

DATAINSPEKTIONEN

HANDLÄGGNINGSLÄGE
1979-03-01

ÄG \ ÅR	1973		1974		1975		1976		1977		1978		SUMMA	
	A	O	A	O	A	O	A	O	A	O	A	O	A	O
11 Principtillstånd	-	-	20	-	6	-	6	3	7	2	3	2	42	7
12 Tillstånd	18	-	2 494	198	925	11	488	9	793	300	615	53	5 333	571
121 Förenkl.	2	-	10 266	68	1 117	15	1 162	6	1 145	23	1 117	138	14 869	250
13 Anmälan	135	5	55	1	9	-	14	-	17	2	6	-	236	8
14 Ändr.	-	-	28	-	115	4	150	2	448	13	282	34	1 023	53
15 Kredituppl. ADB	-	-	3	1	-	-	1	-	2	-	-	-	6	1
16 Kredituppl. ÖVR	-	-	529	3	7	-	3	-	1	-	1	-	541	3
17 Inkasso ADB	-	-	1	-	-	-	2	1	-	-	-	-	3	1
18 Inkasso ÖVR	-	-	214	16	51	9	22	2	23	-	29	13	339	40
19 Övr. tillstånd	1	-	23	-	78	-	83	-	16	1	26	5	227	6
21 Klagomål DL	8	-	67	-	46	-	63	2	45	4	48	8	277	14
22 Klagomål KUL	-	-	14	-	27	-	44	2	80	11	118	18	283	31
23 Klagomål IKL	-	-	16	-	33	1	33	-	65	19	44	19	191	39
24 Initiativ DL	-	-	2	-	3	-	6	1	18	4	13	4	42	9
25 Initiativ KUL	-	-	-	-	1	-	-	-	1	-	2	-	4	-
26 Initiativ IKL	-	-	-	-	1	-	5	2	3	-	2	-	11	2
28 Inspektion	1	-	21	-	63	2	53	4	83	12	53	11	274	29
29 Övr. tillsyn	3	-	58	-	13	1	26	7	26	4	32	12	158	24
71 Adm. ekonomi	16	-	13	-	18	1	12	-	14	1	10	-	83	3
72 Personal	4	-	14	-	6	-	-	-	3	-	-	-	27	-
79 Övr. administration	-	-	4	-	2	-	4	-	4	-	4	1	18	1
81 Remiss	18	-	42	-	48	-	35	-	47	-	49	2	239	2
82 Remiss, besvär	-	-	6	-	18	-	12	-	7	1	5	1	48	2
91 Övr.	14	-	63	1	25	-	16	1	8	2	10	3	136	7
SUMMA	220	5	13 953	288	2 612	44	2 240	42	2 856	399	2 529	324	24 410	1 102

A = Antal ärenden

2.3 Role and significance of the data protection authorities

2.3.0 Introduction

In 2.1 and 2.2 we have shown the rules to which the control authorities must work. At the same time we have given an insight into the mode of operation of a few selected control authorities.

From this material we shall attempt, after a few references to the principal problems of such a project (2.3.1), to reach a few general statements about the role and significance of the control authorities both in the national (2.3.2) and the international (2.3.3) spheres. The impact of control authorities in the further implementation of national and international data protection regulations, especially also with regard to the harmonisation considerations with the EEC, will be of special significance.

It remains to be stressed that in accordance with the pilot nature of the study only preliminary conclusions on this range of problems can be offered, which will need to be refined in the light of further experience.

2.3.1 Analysis Problems

2.3.1.1 Problems of comparability

A comparative summary of the control authorities described runs into a number of diffuculties: such summaries are either not sufficiently detailed to take

The European Parliament has however given a number of recommendations, which indicate a preference for a data protection system based on the Swedish model. The reasons advanced for this are mainly those of adaptability and practicability.

These matters are explored in more detail in 2.4 below. In this connection it may be noted that a simple classification system can cause problems if it ignores the differences between legal systems, whether these are differences in implementation (eg. licencing systems/substantive law), or differences in legal framework and tradition which affect the application of the laws. A more subtle method of approach has, in our opinion priority for the following reason:

- Data protection standards still depend on acceptance by the user and on knowledge by the data subject. They must therefore be rooted in the national context. This arises from the nature of data protecion standards: they regulate the handling of information which needs protection, and through this affect, to a growing extent, all spheres of life- which in turn have their own national variations.

- The existing control authorities still require further experience in their national context. Different forms of control authorities will widen the horizon of experience.

This does not contradict the fact that due to the international aspect of the problem (impact of information technologies on modern industrial societies) international solutions are also possible and desirable. We shall go into this in more detail in 2.5. We are, however, of the opinion that in a study, the aim of which is a better understanding of data protection problems, simple classifications ignore too many of the problems. This does not contradict the fact that on the basis of the regulation material already available, and of previous exprience, some common tendencies can be detected which can form the basis for further development, and from which the requirements of national and international control authorities can be better evaluated. These general observations are set forth in 2.3.2 and 2.3.3.

2.3.2 Role and significance in the national sphere

2.3.2.1 Control authorities as a new type of administration

The control authorities, irrespective of their national form, represent a new type of administration which performs essential control functions in the handling of information which within the national context is regarded as being worth protection. This innovation rests primarily on the roles assigned to them which in the form and in this combination have up to now not been assigned to an organisation. This will be explored in more detail in 2.3.2.2; we would like, however, to refer first to a number of aspects which draw attention to the signifificance of the control authorities.

Dialogue as an operational form

The control authorities have, in general, to give assitance in the application of the data protection law. At the same time they have to enforce the provisions in the most effective and cost-effective way possible. All control authorities must take complaints of data subjects into consideration and at least comment on them. Due to their influence on the implementation and possible amendment of data protection standards, they also have to deal with the points of view of private and public users, of data subjects and their associations, and also with manufacturers. They assist, although at differing levels, in balancing the interests of those who are concerned in the exchange and processing of information. An essential form of working of these control authorities is therefore dialogue - dialogue with scientists of various disciplines who are concerned with this field, dialogue with other control authorities, and last but not least dialogue with their own staff since as a pioneer institution the parties concerned must themselves, work out their scope of activities.

In this case the dialogue with the public has a special importance, greater even than any control function. Consequently all regulations dealt with here provide mechanisms with which the control authorities can refer to the public: the control authorities give comments on data processing in the public and private sectors, regularaly draw up reports for parliament and/or the

government, give advice on drafts of laws which are connected with information tecnology, and serve on relevant committees.

New demands on staff

These functions, which are not mainly standard administrative functions, but essentially combine functions of administration and politics, and are related to a highly-developed technology, make demands far beyond those of conventional administration units. Comparison could perhaps be made with the preparation of policy papers in Ministries. Control authorities differ from these however, (and this leads to intensification of the demands) by a quasi-judicial independence and by far-reaching powers of intervention (in the case of some control authorities anyway).

This has wide-reaching consequences for the demands on their staff.

Because of the dialogue principle, the work must be carried out with rigorous regard to internal communication. In this case it is an advantage that the organisations in their entirety are still relatively distinct. However, it should be recognised above all else that the staff as a whole face a new and different situation and also feel they are sujbected to a strict external control.

With the exception of registration procedures, which are usually formalised, the work of the authorities is, for the reasons discussed above, subject to internal discussion and ad-hoc decision-making. This has led, within the limits of the different national admnistrative styles, to the Authorities adopting less formal and bureaucratic working methods than would normally be the case.

This affects staff recruitment. The heads of the organisations, who are mainly political appointees, have generally been granted the right to take part in staff selection. This recognises that the nature of authorities work requires smooth co-operation within the department. From the specialist point of view however, the job requires a double legal computing qualification. It is true that up to now, formal qualifications have predominantly been in Law. This predominance is not surprising: on the one hand it arises from the function of monitoring the observance of legal regulations and of assisting in the selection of new regulations, on the other hand it is a question of the legally ensured balance of interests, and requires to this extent the socially balancing components of the legal profession.

The necessity of a qualification in computing however, invevitably arises from the nature of the subject. It is an essential basis for competent communication with users, operators, and data subjects.

2.3.2.2 Functions of the control authorities

The new type of functions assigned to these control authorities can be defined as:

- Preventive control
- Acceptance function
- Educative function

Preventive control

The examination of the practice of the control authorities shows clearly that the term control, understood at least as subsequent check, does not go far enough for the description of the actual work of these authorities. In addition to licensing and registration as definite activities, it seems to us that the most important task in the field of control is preventive control.

This preventive control has different outward forms:

While control authorities license and register they also usually prescribe the form of specific systems. Through this they can forestall future dangers by formative regulations.

Where the control authorities on the acceptability of existing systems, these are also used by users, especially large-scale users before systems are

implemented, and quite irrespective whether the control authorities have definite means of sanction or not. This seems to us to be an indication that the philosophy underlying the control authorities, i.e. that of creating acceptance of modern information technologies, is recognised and used (see below).

Insofar that the control authorities have the opportunity of publishing comments or reports (especially in the public sector), these publications also have a preventive effect: by pointing out abuses, generally individual cases, they bring into operation the process of discussion during the course of which not only can the abuse be eliminated, but measures can also be taken to prevent future abuses.

In this connection the regulations of the Land Hesse are to be especially to be pointed out. Together with the obligation of the Land government to comment on the report of the Hessian data protection commissioner, to a certain extent such a discussion process has been made part of the institution. The Commissioner has, moreover, the right to speak in the Hessian Land diet.

This effectiveness of preventive control puts into perspective the impression that the authorities lack effectiveness because of a lack of personnel and consequently limited inspection capability.

Acceptance function

Probably the most important function of the control authorities, quite irrespective of the degree of their powers to intervene, lies in the fact that it seeks to balance the interests of users with those of data subjects. This balancing function can be adequately expressed by stressing the advisory function for users on the one hand, and in the support function for data subjecs on the other. This means that much of the conflict will be settled at the control authorities. The control authority thus becomes a decisive agency for the acceptance by the whole of society of modern information technology. Comparisons with environmental protection authorities and their role in the sphere of industrial chemical and physical technologies become obvious. The problem for the control authorities lies in the fact that their cases of nuisance or "pollution" are, as a rule, "information distribution faults" or "information pollution". These are generally nothing other than the misuse of economic or state decision-making (on the basis of the information handled). The control authorities thus actually tend to become control authorities for economic and political power. Cases of nuisance would therefore not be directly defined as data catastrophies but as misuse of power. At this level, however, the connection with data processing is lost for the data subject and the control atuthorities run into a dilemma: the public is not clear about the ccnnection with information processing and therefore with the actual

sphere of activity of the authority; those causing the situation, who usually understand the connection very well, can use this; the control authorities could either prove no genuine cases of nuisance in their sphere of activity or the objection will be raised that the control authorities have exceeded their powers.

The Swedish example shows, however, how a long tradition of knowledge about the political significance of information (Freedom of the Press Act and the Data Act), can create a climate which has enabled Sweden to become one of the most automated (?) countries.

This acceptance is achieved and will be further advanced primarily by educative work (see below). The requirements are an active information policy, which must exceed the specific legally required reporting, in the form of educational publications and continuous advice.

Educative function

An important part-function within the scope of the acceptance function is therefore the educative function, especially explaining the meaning of data protection. In this respect the control authorities are still faced with difficulties:

Data protection is partly regarded and understood as data security only, i.e. stress is laid on the inaccessibility of the data, without seeing at the same time how

insufficient this is if the application purpose is itself corrupt. The necessity of data protection is partly unrecognised as spectacular cases if misuse have not yet occurred; moreover, it is not recognised that it is exactly at this point of time that qualititatively new problems also arise due to the new information technologies, and that special regulations for the handling of information must be created. It is here that the control authority must be able to show that data protection has preventive functions and only in this way can the application of new technology by democratically checked and controlled. Only such a legitimate accompaniment to technological development enables acceptance of technical development, prevents confidence crises and set-backs in development.

2.3.2.3 Political significance of the control authorities

The growing political significance of the control authorities can be seen in these functions, especially in the overlapping function of ensuring acceptance. There are several reasons for this. In the sphere of information law, to take data protection in its widest, there are still systematised regulations (although they are increasing), and where they exist they are not adequate in every case. The problem of lack of systematisation is exempufied by the unreserved question of the connection between freedom of information and data protection. The position is made worse by the fact that hardly any case law exists on the subject. This means

that in many cases the data protection authorities are entering new territory when they make comments and/or decisions, and for their part must first develop and evaluate their targets. Even where regulations already exists, definite rules of interpretation emerge only gradually, so that even in the interpretation of existing regulations the control authority must first attempt clarification and definition of their targets. This type of discussion and definition is, however, primarily a function of political authorities, of the public (as an institution), of the government and of parliament.

The data protection authorities themselves are therefore close to the arena of political discussion and the political authorities. It is recognised that some of the data protection authorities have a dualistic structure in which political pressure groups (political parties, trades unions, employer associations, the professions etc.) are represented. A further possibility of balance lies in extablishing the data protection authorities in a proper relationship with parliament.

Nevertheless, this development conceals dangers. Due to the political functions just described the decision-making functions can be paralysed. The reasons why signs of this are not yet visible are in part the fact that data protection has not so far really been discussed to any great extent as a party-political issue in the countries concerned. With the growing importance of the subject this situation could alter, however, and it would

be advantageous if political forces in the "second chamber" of such control bodies could mediate in the matter, without at the same time bringing the conflicts into the data protection administration itself. This is especially important in the case of those control authorities which have far-reaching powers of intervention. But there is still a need for the awareness of data protection issues to be imparted from the top downwards. The lack of structure in the area of data protection i.e. in stark contrast to the economic significance of the subject. (In the public sector, efficiency takes the place of profit in the private sector as the motivation for change).

Data processing and information technology have become important factors in the national economy and these technologies are becoming an indispensible infrastructure of national and international markets.

Against this background, knowledge of the actual scope of automated data processing and the international movement of data is becoming more important, even if it at first only concerns data which is within the scope of the specific data protection laws because it is regarded as deserving protection. There is, however, little indication that national governments are consiously aiming to obtain such knowledge by for example, standardising registration obligations in the private sector. This would have the desirable side effect of providing the level of awareness necessary to support the development of national information policies.

There is still little evidence to show to what extent such concepts have been directly converted into decisions of national data protection authorities. The only institution with long experience in the private sector, namely Sweden, cannot yet demonstrate such a general conclusion. Insofar as the control authorities (through comments and recommendations) have come to grips with the general effects of information technology and especially with the effects on power sharing (even if not directly by decisions), the effect of information policy of these control authorities has already shown itself. Such involvement of the control authorities, i.e. intervention on their own initiative in political discussion, cannot be avoided because of the accumulating expert knowledge of the control authorities and should, in general, be encouraged. This should be especially so for questions of harmonisation and of trans-border data flows (see below 2.3.3).

Additional studies would be necessary to further analyse the significance of the control authorities with regard to information policy. Thus, for example, the decisions of the Swedish control authority, especially regarding international movement of data, could be examined to see to what extent criteria are visible in them which go beyond matters of privacy by introducing issues of national sovereignty, security and employment.

In general, however, it can be concluded from the general principle of subordinating the control authorities to the

law and by limiting the law to the relatively narrow field of privacy in the private sphere, that the use of control authorities as agents of national information policy is not to be expected in the immediate future, but this is not to say that the control authorities will not have come to terms with such intentions, and this is a potential area of conflict.

This policical function will become especially clear due to the proximity to questions of national sovereignty in the international field:

Data processing and communications technology do not recognise national boundaries, and indeed, encompass international applications of great importance (e.g. trade). Therefore the international rather than the national level of data protection must be considered. A separate section (2.3.3) has therefore been devoted to the role of the control authorities in this sphere.

2.3.3 Role and significance in the international sphere

Data processing does not stop at state frontiers. Due to the growing significance of the international movement of data in both the private and public sectors, control authorities inevitably have an international significance This international significance arises:

a) from the international functions assigned to it for various reasons,

b) from the existing practice of international co-operation.

2.3.3.1 Control authorities and trans-border data flows

The significance of the international movement of data has already been referred to in section 1 of this study. At this juncture a summary of the relevant regulations and the role of the control authorities in this connection is given.

Belgium

A special control authority for the international movement of data is not envisaged. International data systems are subject to the same criteria as national systems insofar as they come under the jurisdiction of the authority. There is only a special reference to the jurisdiction of the court if the data subject is domiciled abroad.

Denmark

If certain data are not, in general, permitted to be collected in Denmark, then their collection for the purpose of further processing abroad is also not permitted. Systematic data collection at home with the intention of storage abroad is subject to the same licensing conditions and registration obligations as storage at home.

The transfer of sensitive data to foreign countries, and the collection of sensitive data for the purpose of further processing abroad require, in each case, a prior licence from the DSA. In all cases a licence may be granted only if, in the opinion of the DSA, the transfer leads to no material weakening of the position of the data subject as formulated by Danish law.

To fulfill international agreements, or for the purpose of promoting international co-operation, the Minister of Justice can exempt from the obligation of licensing the transfer of data if it is to explicitly named countries or explicitly named data banks abroad. The DSA must be consulted however and the exemption is permissible only if regulations are not jeopardised at national level.

Danish law for the private sector (uniquely among those examined) provisions whereby the relationship of the DSA to other control authorities can be regulated by the Minister of Justice. Thus, for reasons of international co-operation or because of international agreements, arrangements for the supervision of specific users can be made in the registration and licensing procedures, erasure obligations and inspection procedure.

France

Within the framework of applications for registration or opinion, the specifications of the planned information systems must also contain details of whether transfer

abroad will be carried out or not. In addition, transfer can be made subject to approval beforehand, or to special regulations by decree of the Conseil d'Etat by which the maintenance of regulations at the national level is to be ensured.

United Kingdom

The report of the Lindop Committee mentioned trans-border data flows as one essential reason for the necessity of national regulations. Moreover, it proposed that the DPA be given the power to incorporate regulations to cover such transfers in the codes of practice. In this case also the interests of international co-operation and the prevention protectionism masquerading as data protection there should allow modification of codes of practice in order to prevent unreasonable hinderances.

Luxemburg

The law of Luxemburg contains no specific regulations concerning the international movement of data; it does contain, however, by reason of the special situation of Luxemburg, detailed regulations concerning the scope of the law (See 2.1.6).

Netherlands

The scope of the Dutch draft law covers responsible data holders in the Netherlands who store data abroad. Exemptions can be made by the RB if there is adequate protection

By law the RB can also provide exemption from the Dutch regulations if this proves to be sensible in regard to foreign regulations. In addition, the transfer of data to foreign data systems and the receipt of data from such systems is forbidden if this has been forbidden for these systems or these types of systems by statutory rule because of possible danger to the privacy of such persons who are domiciled in the Netherlands.

Federal Republic of Germany

The control system for the Federal Republic of Germany includes trans-border data flow only in regard to the transmission of data from the public sector. This relates in general to laws and international agreements, and to the general regulations that apply to the transmission of data from the public sector within Germany. For the private sector, the same regulations apply whether the transfer is international or within Germany.

Sweden

The licensing law also covers information systems which extend beyond the country's frontiers. The criterion for approval is that the reputation of tne data subject must not be prejudiced by the transmission of the data.

Summary

In summarising, it can be confirmed, that insofar as the Control Authorities have registration and licensing powers, these powers also include trans-border data flow, and therefore the same requirements apply as for the national systems. Where trans-border systems are specifically mentioned in the legislation or in the drafts, the deciding criterion for approval is the maintenance of the relevant national standard of data protection. This criterion is also to be found in the data protecion laws, which directly govern only the national circulation of data but which implicitly also apply to the transmission out of the country.

Major problems are however encountered in detecting dangers to the national control standard. (Here also lies a series of problems for international agreements, which on the one hand aim to facilitate the exchange of data between the partners to the agreement, which on the other hand the data protection standard in relation to ouside countries is to be safeguarded). Where a data protection law is in force in the receiving country, this in itself is normally still no guarantee that no danger exists, as this law has to be checked in the first place. Even when there is no special data protection law in force in the receiving country, this does not recessarily preclude the transmission of data, as all legal regulations have to be checked in the inquiry with regard to the control standard. This faces the Control

Authority with a difficult task in respect of legal comparison which has serious practical consequences. One has only to consider the exchange of data with countries such as the USA and Canada, which have no general federal data protection leglislation for the private sector. International agreement in this area will become vital in the future as will further investigation from which decisions, particularly those which have already been reached by the Data Protection Control Authorities such as Sweden, can be analysed (see 2.5). This leads to consideration of the existing practice and the possible role of the Control Authorities in the international sphere.

2.3.3.2 International co-operation of thh Control Authorities

Reasons for international co-operation

The preceding section indicated one of the possible duties of the Control Authorities in the international field and the importance of international co-operation.

The necessity for international co-operation stems directly from the international range of the subject, but also inevitably from the functions of the data protection Control Authorities in the national sector.
In particular:

No existing data protection law includes an express mandate for international co-operation. The most explicit, besides the Danish Law already discussed, is

the Norwegian law: with a directive to the effect that co-operation with other Data Protection Authorities can be regulated by legal decree. However, before going into this probem and its solution in greater detail, the duties involved in such international co-operation will be presented in more detail.

One duty evolves from the previously-described problems of trans-border data flow, and the difficulty of obtaining information on the relevant standard of control. The Control Authorities evidently agree that the degree of compatibility of the various national data protection laws needs clarificiation.

A further area of co-operation arises from the acceptance function of the Control Authorities. A user of tans-border data systems must be informed at the earliest possible moment of the relevant national control requirements and the problems involved in the crossing of the frontier. This particularly applies to users who operate in several countries. The Control Authorities in agreement with one another, must be able to advise about other countries' requirements.

Such internationally-agreed consultation within the framework of the acceptance function must however, above all, be capable of working to the advantage of the data subjects who, as a general rule, become familiar with the national data protection system only by degrees, and who need the assurance that their rights are safeguarded

outside their own country. In this, the data subject needs to be able to contact the foreign Control Authority directly or, which is more probable, to approach the national Authority with which he is rather more familiar, who will then contact the foreign organisation on his behalf. Timesaving, inexpensive procedures need to be developed in this area.

Difference in the scope of the various national authorities should not work to the disadvantage of the data subject, and the Control Authorities should make internal arrangements in respect of the supply and transmission of information to data subjects.

In comparability problems like this, which are always arising in data protection, the Control Authorities must find a way to continually exchange experiences.

None of the above-mentioned international functions is at present explicitly ascribed to the Control Authorities, but even without a general formal ruling, a practice of co-operation has already evolved.

Practice of international co-operation

This resulted in the first place from the creation of the respective national data protection laws. Countries which already had data protection legislation in force have provided the newcomers with substantial assistance

in compiling regulations, in their implementation and in establishing the institutions. The Authorities of Hessen and Sweden, with their experience of data protection, played a distinctive part in this respect. This co-operation in development has led to co-operation n practice, and to the laying of a foundation for a continuous interchange of experiences.

In this way collaboration of between Control Authorities, and with users and data subjects, has further developed. An influential factor in this has been the recognition, in national discussions of foreign regulations and practices, that the problems which have to be dealt with, the social situations in which they occur, and the technical aids which are available, are similar, despite the different legal and constitutional frameworks into which the solutions must be fitted.

In this connection, the first conference of the national Control Authorities was held in Bonn on May 3/4 1979. With the exception of New Zealand (prevented through urgent official duties), all countries were represented which had established a Control Authority for their data protection laws, namely: Canada, Denmark, France, Sweden and West Germany.

This first conference served essentially to establish initial personal contacts and a better understanding of the Control Authorities concerned. Nevertheless, subjects from the described international functions of the Control Authorities were dealt with:

- problems of trans-border data flow,
- problems of data subjects,
- international information systems holding personal data. F1

This conference must be regarded as an important step towards a harmonisation of the data protection regulations, and above all, data protection in practice. This development is moreover, taking place in parallel with the preparations for the implementation of international law in the field of data protection. It appears to us to be of particular importance, that non-European countries are also participating.

This leads to the demands which can be made on the Control Authorities as a result of international agreements, or the drafts of such agreements, and particularly to the possible consequences which could ensue from resolutions of the European Parliament.

(Footnote 1: The next conference is expected to take place in Canada in 1980).

2.4 Future demands on the Control Authorities in the European Economic Community and their feasibility

2.4.1 Recommendations of the European Parliament

A resolution on the protection of the rights of the individual in the face of technical developments in data processing (published in the Official Journal of the European Communities no. C 140 of 5 June 1979), the European Parliament, referring to the Control Authorities, stated:

"The European Parliament ...
Considers it essential that, without prejudice to the Commissions supervisors powers as guardian of the Treaties, a committee of representatives of the national bodies of the Member States responsible for the application of the legislation, general or specific, relating to the protection of liberties, be instructed to supervise the implementation of Community texts and ensure the smooth functioning of the cooperation required between those bodies; Considers it necessary that the European Parliament be appropriately represented on and hold the chairmanship of this committee and that the committee should report to the European Parliament and to the Commission and Council;"

The Commission and the Council are strongly urged to take into consideration the following principles relating to the Control Authorities, which can be issued as a Community regulation on data protection:

- The appointment of an independent body with appropriate staff and funds by each of the Member States, for supervising the Community regulations and the internal regulations of the individual States.

- The national data protection bodies should supervise the following functions as a minimum:

  a) appropriate publication of registered data banks,
  b) informing the public of their rights,
  c) assistance in exercising these rights,
  d) the keeping of a register, which may be inspected on proof of a legitimate interest,
  e) an annual report to the data control body of the European Community.

- The transmission of personal data within the Community is to be notified to the European Data Protection body (see above). (The data is not to be subjected to any special control beyond this.) Authorization by the data control body of the European Community is required for the export of data ouside the members of the Community. For its part, the European Data Protection body will compile an annual report for the European Parliament.

The legal problems (range of jurisdiction of the EEC treaties, inclusion of the public sector, distortion

of competition, etc.), will not be considered here. F1

In its questionnaire on the preparations for the public hearings with regard to data processing and personal rights in Brussels on February 6th 1978, the Sub-committee 'Data Processing and Personal Rights' of the European Parliament Legal Committee wished to know, inter alia, whether a separate Control Authority would be required for the control of data protection within the European Community and how this was to be organised (see Question IV(4) European Parliament PE 56.386/Anl.I/endg.).

The response of the experts to this query was somewhat reserved. In its report, the Sub-committee summarized the views of the experts as being to the effect, that instead of a supervisory authority at Community level, possibly a framework for intenational co-operation could be produced. Contacts should then be made between data protection authorities in an Advisory Committee, in which manufacturers, users and data subjects would participate. F2 Nevertheless, the above-mentioned recommendations were accepted by the European Parliament, were again fully confirmed and at its meeting on September 24th 1979.

(Footnote 1: refer to the experts of the EEC legal Service, SEC(77)3176 and III/1540/79 DE, also European Parliament PE 49.541/Anm.4 and PE 49.822/rev.)
(Footnote 2: European Parliament PE 56.386/Anl. I/endg. No. 14d).

2.4.2 Consequences

2.4.2.1 National Control Authorities

The effects of this recommendation are not at present, foreseeable, particularly because all EEC countries do not yet have data protection laws.

On the basis of this study however, a number of findings can already be established with regard to the demands on the national Control Authorities:

1. Each of the laws or proposals covered in this study involves a Control Authority or makes provision for one even if with varying powers.
2. Each of these Control Authorities keeps a register, or is to keep such a register, which can be perused.

In respect of trans-border data flow however, special conditions for approval exist within the European Community, (refer to 2.4.2 above). It is to be doubted if counties which already have data protection legislation in force will depart from the approval stipulations laid down therin, until a more uniform standard of regulations have been achieved within the Euorpean Community. F1

(Footnote 1: This position is also legally problematical, see 'EEC Commission, Service Juridique III/1540/79 DE.)

Consequently, with regard to the demands of the European Parliament on the national Control Authorities, at the present time there only exist problems concerning trans-border data flow (apart from the problem that not all the countries within the EEC have data protection laws in force).

These problems have however been largely resolved, as in this sector international co-operation, particularly within the framework of contact between the Data Protection Authorities , has just begun, (see 2.4.2.2). Such agreements have also been possible, in individual cases, with those EEC countries which have no data protection legislation.

2.4.2.2 The European Data Protection Body

The European Parliament has however, as explained, also proposed the establishment of a European Data Protection Body.

On the basis of this present study however, in our view, under the present circumstances, standardisation of the organisational structure of the Control Authorities and their incorporation into a European Data Protection Body is not to be considered. This opinion results directly from the described functions (2.4.1.2) of the Control Authorities in both the national and international sectors (2.4.2).

The most important function of the national Control Authorities at present, is to provide for a climate of acceptance of data protection. The already complex structure of regulations and responsibilities for users and data subjects would become even more complicated with the creation of a new authority at the present time. An effective supra-national administration of data protection pre-supposes its acceptance at national level, an acceptance however, not only by regulation but also in practice.

In their varying forms of incorporation, authority and procedure, the Authorities are adapting to the national political and legal characteristics of data protection. In future these Authorities, in their national context, need the recognition of the public, who must be able to turn to them with a certain degree of confidence. The educational potential of the authorities is dependant on their public image, therefore any changes to the authorities which may affect this image, will have a more adverse effect than would changes to these detailed procedures. It would in any case be large users with systems in a number of EEC countries who would profit directly from the advisory function of a higher EEC Control Authority. Such large users normally have equipment at their disposal which enables them to solve multilateral legal problems and to keep in contact with the different national Control Authorities.

This does not rule out the possibility of the Control Authorities in their present constitutional form being the carriers of legalistic adaptation procedures, and they can also perform an implementation function in European, and not only national, data protection.

The Control Authorities can perform this function, particularly in their every-day practice, i.e., in their advisory and assistance capacity for data subjects and users.

The enforcement function is in any case, of minor importance at the present time, and this applies even more to the international sector.

Moreover, the Control Authorities, certainly in the national territories, must be allowed to continue and extend the practice of their international co-operation, even beyond the EEC. This can come about by these functions being given explicit consideration in forthcoming legislation, and also where this is not needed at least in the provision of resources, in the internal organisation and in recruiting, adequate consideration should be made. Should restrictions exist to any extent, then these should be removed.

This does not rule out a particularly close co-operation with the EEC by the Control Authorities. Such co-opration may be regarded as a preliminary stage twoards a European Control Authority. This co-operation is

however of such importance in the EEC zone, (avoiding distortion of competition, safeguarding the living standards of the EEC citizens), that it must be ensured through an appropriate mechanism, that data protection problems in an exchange with outside countries, and also the problems of the developing countries, are not lost sight of in the process. Just as the problems of trans-border data flow do not completely end at the frontiers of the countries concerned, so do they also not come to an end at the frontiers of the EEC countries. The danger would otherwise very easily exist of the same problems arising in the near future at the frontiers of the EEC, which at present exist at the frontiers of the member states.

An adequate solution of these problems however, goes far beyond the scope of this preliminary investigation and would have to be the subject of further research activity (2.5).

Special co-operation within the EEC is however of importance to the extent that it is possible, and in our view also necessary, for the European Parliament to become involved.

In other words, should a particularly close co-operation develop over a long term between the Control Authorities of the EEC, and such co-operation be institutionalised in some manner (such institutionalisation could take place in an initial stage as in the Convention Draft of

the European Council -CJ-PD(79)MISC 7 of 24.5.1979 - Art. 13), then the European Parliament should participate therein through a Consultative Panel. This resulls from the growing political function of the Control Authorities, to which we have previously referred (2.4.1.3). These political functions also exist in the international sector. To the extent to which the collaboration of the Control Authorities creates an international practice, it will also be necessary for such an evolving practice to be controlled politically and legitimised democratically. The participation of the European Parliament in these developments therefore, appears to us to be desirable, not least in regard to the functional efficiency of the national Control Authorities. Furthermore, a number of problems arise in the field of information technology in the relationship of Parliament to Government. These are problems which Fl will also affect the European Parliament in the long-term in its standing to the other organisation of the Community. This development will however depend on the future political and legal role of the European Parliament.

(Footnote 1: This has only partly been taken into consideration in data protection legislation, eg., in Hessen (1.2.2.1) and Luxembourg (1.2.1.6), problems of covering information requirements and the distribution of information on a background of a functional division of the political powers).

Irrespective of any such development, further functions of the Control Authorities should be promoted within the framework of the EEC. This particularly applies to the educational function of these Authorities, previously referred to. The supervision of this function within the EEC merits special support from the Community organisations in the interests of the economic conditions in the EEC. This educational function is the crucial principle for a long-term safeguarding and implementation of regulations for the socially responsible treatment of information, particularly since as previously explained, sanctions in this connection are only of secondary importance. Problems for both the user and the data subject will arise internationally to an increasing extent, particularly in view of the creation of international data networks, not least in the EEC. The support of the responsible organisations of the EEC is therefore essential if co-operative efforts in this sphere are a clear insight into the problems fo trans-border data flow, and so by example effect assurance and understanding, and therefore acceptance. F1

(Footnote 1: as an example of co-operation in his area, it should be ppossible, within a suitable time-scale, to produce a Users' Handbook containing relevant information for the setting up, within the EEC, of databanks containing personal data).

2.5 Possible Keypoints for Future Research

2.5.0 Preliminary Remarks

This investigation was a preliminary study. It had value in revealing first of all the multiplicity of problems concerned in the differing data protection regulations, particularly within the European community, from a selected number of crucial points. One such point was considered to be the role of the Control Authorities. Development is progressing simultaneously, drafts of international agreements are in hand, but have not yet been concluded. Not all the countries of the EEC have data protection laws. The international and national regulations are in need of conversion. In other countries, amendments have already taken place or are imminent. On account of the great importance of information processing, this development requires intensive scientific attention to be applied to it. This particularly applies to the observation of the practice of the Control Authorities.

In the following pages therefore, possible crucial points for future research will be presented. These developed from the work on this part of the present study, which revealed some aspects of the topic which could not be covered in full depth. These are discussed further in 2.5.1. Other points arose from areas closely related to the present study, which have had to be omitted at this stage, but obviously merit attention in future. These are covered in section 2.5.2.

2.5.1 Crucial points within the scope of the present study

The practice of the existing and future Control Authorities within the European Community needs further investigation. In this connection, it is particularly desirable to discover whether, and to what extent, different regulations lead to significantly different results, that actually affect in day-to-day practice in EDP. This distintion between the regulations and their effects appears to us to be necessary, because the existing regulations contain numerous exclusion conditions and delegation standards and the Control Authorities develop different interpretation practices, so that on the basis of the regulation alone, the effects can no longer be adequatelyy evaluated. In this connection, an analysis should be made, particularly of the Control Authority's recommendation and decision-making duties, in order to obtain a comprehensive picture of data protection in action, and to permit statistical comparisons of the organisational patterns.

Special consideration has to be given to the practice in the international sector in this inquiry, in order to determine the extent of the progress of an effective harmonisation and how much influence on this practice international agreements have, or could have.

In the international field, priority should be given to dealing with the question of what part will be played by the Control Authorities in information relations with countries outside the European Community.
countries outside the Euopean Community.

2.5.2 Related problems

Among the problems which lie outside the scope of this inquiry, but which stand in close relationship to the Control Authorities, the effects of the harmonisation proposals of the European Parliament, and the international role of the Control Authorities outside the area of data protection in its strict sense, would be primary subjects for investigation.

For this, inquiries should be made into the feasibility of an EEC Control Body, particularly its organisational make-up, the nature of the co-operation, with the national authorities, and the potential inluence of such an authority (including its relations with countries outside the EEC).

Within this international sphere, priority should be given to the role of the Control Authorities in international research (clearing station for European research planning), their role in information distribution (mainly between developed and developing countries), and the investigation of their educational function, particularly for the citizens of the Community.

2.6 Bibliographie

(1) Anderson, Margaret L.B.:
The Forthcoming data protection Legislation:
A Talk by Paul Sieghart.
In: Computer and Law 9(1976) S.5-6

(2) Andrews, W.H.:
An Overview of the Emerging Statutory "Right"
of Information Privacy.
In: Law and Computer technology (1977) H.4
S.82-94

(3) Aner, K.:
The New Swedish Data Act.
In: Transnational data regulation.
Proceedings OnLine conference Brussels 1978

(4) Auernhammer, Herbert:
Der Regierungsentwurf eines Bundes-Daten-
schutzgesetzes.
In: OffentLiche Verwaltung und
Datenverarbeitung 4(1974) H.3 S.51, 123ff

(5) Auernhammer, Herbert:
Die Konzeption des Entworfs des Bundesdaten-
schutzgesetzes unter besonderer Berucksich-
tigung des betrieblichen Datenschutzbeauf-
tragten. Dortmund 1974.
In: Der Datenschutzbearftragte: Gesetzliche
Anforderungen und Erfahrungen in der Praxis, S.17-31

(6) Auernhammer, Herbert:
Datenschutzgesetzgebung - Magna Charta des Burgers von heute.
In: Krauch, Helmut (Hg.): Erfassungsschutz.
Stuttgart 1975, S. 57 ff.

(7) Auernhammer, Herbert:
Bundesdatenschutzgesetz - Kommentar.
KoLn 1977

(8) Auernhammer, Herbert:
Das Bundesdatenschutzgesetz.
In: Betriebsberater (1977) S.205

(9) Auernhammer, Herbert:
Basic issues in data protection legislation and its international harmonisation.
In: OECD, ICCP Vol. 1, Paris 1979, S.298-301

(10) Avison, D.E.; Crowe, T.:
Computers and Privacy.
In: Computer Bulletin, March 1976, pp. 8-13

(11) Banques de donnees, Entreprises, Vie privee:
Conference Proceedings.
Namur 1979

(12) Bartsch, H.-J.:
Die Entwicklung des internationalen Menschenrechtsschutzes im jahre 1977.
In: Neue Juristische Wochenschrift 31(1978) H.10 S.449-445

(13) Barthelemy, M.J.:
Das belgische Nationalregister.
In: Offentliche Verwaltung und Datenverarbeitung 2(1972) S.141-144

(14) Bastin, J.:
Les flux des donnees transfrontieres dans le domaine de l'assurance-credit.
In: OECD, ICCP Vol. 1,Paris 1979, S. 127-132

(15) Bayerl, Alfons:
Bericht uber den besuch beim schwedischen Datenuberwachungsamt, 23. und 24. Januar 1979.
Europaisches Parlament, RechtsausschuB, "Datenverarbeitung und Personlichkeitsrecht", Dokument PE 56.958/Anl. 1, 30.1.1979, 6pp.

(16) British Computer Society, Pruivacy Committee:
Submission of Evidence to the Committee onPrivacy (Younger Committee).
March 1971, 25 pp.

(17) British Computer Society:
Submission of Evidence to the Data Protection Committee (Lindop Committee).
October 1976, 31pp + appendices

(18) Beckler, D.:
Closing remarks.
In: OECD, ICCP Vol. 1, Paris 1979, S.318-320

(19) Benjamin, A.,A.:
Privacy, Security and Responsibility.
In: Transnational data regulation.
Proceedings Online comference Brussels 1978.
S. 1-8

(20) Benjamin, A. A.:
Privacy and computers.
In: OECD, ICCP Vol. 1, Paris 1979, S.174-177

(21) Bergmann, Lutz; Mohrle, Roland:
Datenschutzrecht. Handkommentar zum Bundesdatenschutzgesetz.
Stuttgart/Hannover/Munchen 1977

(22) Bergmann, Lutz:
Datenschutzaufsicht in den Landern - Auswirkungen auf die Wirtschaft.
In: Datenschutzkongre '79, Berlin, 11.-13 Juni 1979. Dokumentation, I/3 (B)

(23) Bernhard; Gola; Tuner:
Ubersetzung des franzosischen
Datenschutzgesetzes.
In: Datenschutz und Datensicherung (1978)
S.157

(24) Bernasconi, F.,A.:
National Information Policies to Determine
Transnational Data Regulation.
In: Transnational data regulation.
Proceedings Online conference Brussels 1978,
S.9-14

(25) Bernasconi, F.A.:
Informatics integral to a new international
economic and information order.
In: Data Regulation European and Third World
Realities, Conf. Proc., S.113-122

(26) Der Bundesbeauftragte fur den Datenschutz:
Was bringt das Bundesdatenschutzgesetz? Eine
Information fur den Burger.
Bonn 1978

(27) Der Bundesbeauftragte fur den Datenschutz:
Erster Tatigkeitsbericht.
Bonn 1979
(Auch abgedruckt in: Bundestagsdrucksache
8/2460)

(28) Bing, J.:
Transborder Data Flows - Some Legal issues and Possible Effects on Business Practices.
In: Transnational data regulation.
Proceedings Online conference Brussels 1978, S. 15-28

(29) Bing, Jon:
A Comparative outline of Privacy Legislation.
Comparative Law Yearbook, 2(1978), p.149 - 181

(30) Birkelbach, Willi:
Das hessische Modell des Datenschutzes.
In: IBM Nachrichten (1974) H.222 S.249

(31) Bundesministerium des Innern (Hg.):
Dokumentation einer anhorung zum Referenten - entworf eines Bundes-Datenschutzgesetzes vom 7.-9. November 1972.
Bonn 1973

(32) Bode, Albrecht; Drews, Hans-Ludwig:
Die Auswirkungen des BDSG in der Industrie.
Siemens Aeitschrift Nr.5 (1977) S.370ff

(33) Bundesregierung:
Entwurf eines Gesetzes zum Schutz vor Mi brauch von personenbezogenen Daten bei der Datenverarbeitung (Bundesdatenschutzgesetz - BDSG).
In: Bundesratsdrucksache 390/73

(34) Bull, Hans Peter:
Entscheidungsfragen in Sachen Datenschutz.
In: Zeitschrift fur Rechtspolitik 8(1975) H.1 S.7 ff.

(35) Bull, Hans Peter:
Das Bundesdatenschutzgesetz in der ersten Phase seiner Verwirklichung.
In: Offentliche Verwaltung und Datenverarbeitung - Online - ADL-Nachrichten (1978) H.8 S.572

(36) Burkert, Herbert; Fiedler, Herbert:
Datenschutz und Europaische Gemeinschaft.
In: Das Parlament 28(1978) H.34 S.14 ff

(37) Burkert, Herbert:
Europarat und Datenschutz.
In: Datenschutznachrichten (1978) H.1

(38) Burkert, Herbert:
Europaisches Parlament, EG-Kommission und Datenschutz.
In: Datenschutznachrichten (1978) H.2

(39) Carmody, F.:
The work of the European Community in the area of computers and privacy.
In: Data Regulation European and Third World Realities, Conf. Proc., S.105-112

(40) Carmody, F.:
The Role of the European Parliament in Data Protection.
In: OECD, ICCP Vol. 1,Paris 1979, S.231-232

(41) Committee of Privacy:
Report of the Committee on Privacy. Chairman: Sir Kenneth Younger.
Her Majesty's Stationary Office, Cmnd. 5012, London, July 1972, xi + 350 pp.

(42) Commission Informatique et Libertes:
Rapport de la Commission Informtique et Libertes, tome 1.
Paris 1975
106 pp

(43) Commission Informatique et Libertes:
Rapport de la Commission Informatique et
Libertes, Annexes, tome 2.
Paris 1975
446 pp

(44) Committee on Data Protection:
Report of the Committee on Data Protection.
Chairman: Sir Norman Lindop.
Her Majesty's Stationary Office, Cmnd.7341,
December 1978, xxiv+460 pp.

(45) Commission Nationale de l'Informatique et
des Libertes:
Rapport sur la Commission Suedoise
d'Inspection des Donnees par L.Joinet et
F. Bancilhon.
Paris 1979 1979

(46) Delbetankande av datalagstiftingskomitten
(DALK):
Personregister Datorer Integritet.
Stockholm 1978
(English Summary pp. 337-363)

(47) Dammann, Ulrich:
Datenschutzkontrolle - Bericht aus der Praxis
eines Landesbeauftragten fur den Datenschutz.
In: IBM Nachrichten (19) H.236 S.187

(48) Dammann, Ulrich; Karhousen, Mark; Muller, Paul; Steinmuller, Wilhelm:
Datenbanken und Datenschutz.
In: Bellebaum, Alfred (Hg.): Soziale Probleme. Frankfurt; New York 1974

(49) Dammann, Ulrich:
Der Datenschutz in der Praxis - die Erfahrungen des Hessischen Datenschutz - beauftragten.
In: Datenverarbeitung im Recht Bd. 5(1976) H.1/2 S.41-52

(50) Dammann, Ulrich; Simitis, Spiros:
Bundesdatenschutzgesetz mit Materialien.
Baden-Baden 1977

(51) Dammann, U.:
Anwendungsmatrix des Bundesdatenschutzgesetzes.
In: Online adl-Nachrichten (1977) H.1/2 S.74-80

(52) Dammann, U.:
Die Kontrolle des Datenschutzes. Eine Untersuchung zur institutionellen Kontrolle des Datenschutzes im offentlichen Bercich Kybernetik. Datenverarbeitung. Recht 7, Frankfurt a.M. 1977

(53) Dammann, Ulrich; Mallmann, Otto; Simitis, Spiros:
Data protection legislation. An International Dokumentation. Die Gesetzgebung zum Datenschutz. Eine internationale Dokumentation. Englisch-Deutsch.
Frankfurt / M 1977
In: Forschungsstelle fur juristische Dokumentation (Hg.): Kybernetis, Datenverarbeitung und Recht. Band 5

(54) Dammann, Ulrich:
Die Kontrolle des Datenschutzes im offentlichen Bereich.
In: Kybernetik, Datenverarbeitung im Recht Bd.7

(55) Dammann, Ulrich:
Transparenz der Datenverarbeitung - Erfolge und Defizite.
In: Datenschutzkongre '79, Berlin, 11.-13 Juni 1979. Dokumentation, I/3 (A)

(56) DeMaio, H.B.:
Transnational information flow - a perspective.
In: Data Regulation European and Third World Realities, Conf. Proc., S.169-178

(57) Donovan, J.F.:
Problems of privacy.
In: Diebold Research Program-Europe, Data Exchange, May-June 1977, pp. 18-20

(58) Dreyfous, E:
Le commerce international et le flux des donnees transfrontieres.
In: OECD, ICCP Vol. 1, Paris 1979, S.81-85

(59) Eger, J.M.:
Alliance for World Communications.
In: Transnational data regulation.
Proceedings Online conference Brussels 1978
S. 33-40

(60) Egloff, Willi; Schimmel, Wolfgang:
Die "Magna Charta des Burgers von heute"?
Anmerkungen zum neuen Bundesdatenschutzgesetz.
In: Demokratie und Recht 5(1977) H.2
S. 124-138

(61) Eriksson, A:
The Vulnerability of Society.
In: Transnational data regulation.
Proceedings Online Conference Brussels 1978.

(62) Fiedler, Herbert:
Datenschutz und Gesellschaft.
In: Stinmuller (Hrsg.): Informationsrecht und Informationspolitik, Munchen 1976, S. 179ff.

(63) Fiedler, Herbert:
Datenschutz und Datenverarbeitungstechnik.
In: GMD-Spiegel 7(1977) H.4 S.51-60

(64) Fiedler, Herbert:
Vom Datenschutz zum Informationsrecht - ein Beitrag aum Thema Datenverarbeitung und Gesellschaft.
In: GMD-Spiegel 7(1977) H.3 S.23-33

(65) Fishman, William, L.:
International Data Flow: Some Brief Thoughts on the View from the United States.
In: Transnational data regulation.
Proceedings Online conference Brussels 1978.
S.41-46

(66) Focus on France.
In: Transnational Data Report Vol. 1(1978) No.1 pp.1-8

(67) Focus on Germany.
In: Transnational Data Report Vol. 1(1978) No.2 pp.1-2, 15-21

(68) Focus on Norway and Sweden.
In: Transnational Data Report Vol. 1(1978)
No.3 pp.1-6, 14-16

(69) Focus on Denmark.
In: Transnational Data Report Vol. 1(1978)
No.4 pp.1f,4f,8,12

(70) Focus on United States.
In: Transnational Data Report Vol. 1(1978)
No.7pp.1-2,12

(71) Focus on United Kingdom.
In: Transnational Data Report Vol. 1(1978)
No.8pp.1-4,10-14

(72) Freese, J.:
Das Schwedische Datengesetz.
In: Aktuelle Informationen aus Schweden
Nr.178, Stockholm 1977

(73) Freese, J.:
The Swedish Data Act.
In: Transnational data regulation.
Proceedings Online conference Brussels 1978.
S. 197-208

(74) Freese, J.:
The present and future Swedish Data Policy.
In: Data Regulation European and Third World
Realisites, Conf. Proc., S.71-84

(75) Freese, J.:
The Swedish Data Act.
In: Review Briefings Eurocomp78,
online-conference, London 1978.

(76) Freese, J.:
Preserving the open flow of information
across borders.
In: OECD, ICCP Vol 1, Paris 1979, S.280-287

(77) Frosini, Vittorio:
Der Burger und der Computer in der
italienischen Rechtspraxis.
In: Datenverarbeitung im Recht Bd. 2(1973)
H.2/3 S.195-206

(78) Garstka, Hansjurgen:
Grundbegriffe fur den Datenschutz.
In: Kilian u.a. (Hg.): Datenschutz. Frankfurt
1973, S.209 ff.

(79) Garzon, G.:
Information and privacy protection in transborder
data flows: the rights involved.
In: OECD, ICCP Vol. 1,Paris 1979, S.302-307

(80) Gassman, H.P.:
The activities of OECD in the field of
transnational data regulation.
In: Data Regulation European and Third World
Realities, Conf.Proc., S.177-184

(81) Gassmann, Hans Peter:
Kunftige Internationale Datenschutzregelungen und ihre Auswirkungen auf die Praxis.
In: Datenschutzkongre '79, Berlin, 11.-13-Juni 1979. Dokumentation, II/7

(82) Gassmann, H.P.:
New international policy implications of the rapid growth of transborder data flows.
In: OECD, ICCP Vol. 1,Paris 1979, S.51-61

(83) Geiger, Hansjorg:
Datenschutz in der Schweiz und anderen Demokratien.
In: Datenverarbeitung in Steuer, Wirtschaft und Recht (1978) H.5 S.120

(84) Geller, H.:
Policy implications concerning international data networks.
In: Data Regulation European and Third World Realities, Conf.Proc., S. 13-16

(85) Gliss, Hans:
Ein Jahr Datenschutz-Praxis - Der Datenschutzbeauftragte heute.
Bonn 1979
In: GDD (Hg.): Datenschutzfachtagung DAFTA '78. Tagungsband, S. 9-14

(86) Gesellschaft fur Mathematik und Datenverarbeitung
(Hg.):
Auswirkungen des Datenschutzes. Eine Studie zum
Datenschutz.
Munchen 1979.

(87) Gola, Peter; Hummerich, Klaus; Kerstan, Uwe:
Datenschutzrecht. Erlauterte Rechtsvorschriften und
Materialien zum Datenschutz Teil 1.
Berlin 1977
In: EDV und Recht 10 Teil 1

(88) Gola, P.; Hummerich, K.; Kerstan, U.:
Datenschutzrecht.
Teil 2: Einzelvorschriften des Bundes zum
Datenschutz.
Berlin 1978.

(89) Goldwater, B M.:
Transnational Data - Facing Realities.
In: Transnational data regulation.
Proceedings Online conference Brussels 1978,
S. 227-232

(90) Groben Wolfgang von der:
Anforderungen der Aufsichtsbehorden an die
Ordnungsma igkeit des Datenschutzes.
Bonn 1979
In: GDD (Hg.): Datenschutzfachtagung DAFTA '78.
Tagungsband, S. 61-72.

(91) Hellner J.:
Datenschutz in Schweden.
In: Festschrift fur Reimer Schmidt. 1976,
S.265-283

(92) Henze, Dirk:
Grundsatze zur Datensicherung in der
Bundesverwaltung.
In: Datenschutz und Datensicherung (1978) H.1
S.31

(93) Hessischer Landtag:
Vorlage des Datenschutzbeauftragten
betreffend den Ersten Tatigkeitsbericht.
Landtagsdrucksache 7.1495. 1972

(94) Hessischer Landtag:
Stellungnahme der Hessischen Landesregierung
zum Ersten Tatigkeitsbericht des Datenschutz-
beauftragten.
Landtagsdrücksache 7/1705. 1972

(95) Hessischer Landtag:
Vorlage des Datenschutzbeauftragten
betreffend den Zweiten Tatigkeitsbericht.
Landtagsdrucksache 7/3137. 1973

(96) Hessischer Landtag:
Vorlage des Datenschutzbeauftragten
betreffend den Dritten Tatigkeitsbericht.
Landtagsdrucksache 7/5146. 1974

(97) Hessischer Landtag:
Vorlage des Datenschutzbeauftragten
betreffend den Vierten Tatigkeitsbericht.
Landtagsdrucksache 8/438. 1975

(98) Hessischer Landtag:
Vorlage des Datenschutzbeauftragten
betreffend den Funften Tatigkeitsbericht.
Landtagsdrucksache 8/2475. 1976

(99) Hessischer Landtag:
Vorlage des Datenschutzbeauftragten
betreffend den Sechsten Tatigkeitsbericht.
Landtagsdrucksache 8/3962. 1977

(100) Hogrebe, Edmund F.M.:
Verwaltungsautomation und Datenschutz in
Frankreich.
In: EDV und Recht Bd. 9. Berling. 1976-649 S.

(101) Hogrebe, Edmund F.M.:
Das franzosische Datenschutzgesetz.
Ubersetzung des Gesetzestexts.
Kurten 1978
Selbstverlag

(102) Hogrebe, Edmund F.M.:
Second Look at Implementing the German Data Protection Act.
In: Transnational Data Report Vol. 1(1978) No.3 pp.9-12

(103) Home Office:
Computer and Privacy. (White Paper).
Her Majesty's Stationary Office, Cmnd. 6353, London December 1975, 13 pp.

(104) Home Office:
Computers: Safeguards for Privacy (Report).
Her Majesty's Stationary Office, Cmnd. 6354, London December 1975, 48 pp.

(105) Hondius, F.W.:
The Council of Europe's Data Protection Principles.
In: Transnational data regulation.
Proceedings Online conference Brussels 1978, S. 47-54

(106) Hondius, F.W.:
The work of the Council of Europe in the area of data protection.
In: Data Regulation European and Third World Realities, Conf.Proc., S. 59-70

(107) Hondius. F.:
The action of the Council of Europe with regard to international data protection.
In: OECD, ICCP Vol. 1, Paris 1979, S. 257-260

(108) Hummerich, Klaus:
Das Bundesdatenschutzgesetz.
In: Juristische Schulung (1977) S.272

(109) Deutsche Sektion der internationalen Juristen-Kommission (Hg.):
Datenschutz und Datensicherung. Vortrage.
Karlsruhe 1975

(110) Janson, C.-G.:
Privacy Legislation and Social Research in Sweden.
In: Proceedings. International Conference on Emerging Data Protection and Social Sciences' Need for Access to Data.Koeln 1978

(111) Joinet. L.:
French Law in relation to information on card indices and liberties.
In: Data Regulation European and Third World Realities, Conf.Proc., S. 215-222

(112) Joinet, L.:
Les aspects juridiques, economiques et sociaux des flux transfrontieres des donnees personnelles.
In: OECD, ICCP Vol. 1, Paris 1979, S. 208-212

(113) Jordon, A.S.:
Summary of the Position in the United Kingdom.
In: Review Briefings Eurocomp 78, online-conference, London 1978

(114) Kamlah, Reprecht; Schimmel, Wolfgang; Schwan, Eggert; Haenschke, Frank:
Kommentar zum Bundesdatenschutzgesetz.
Berlin o.j.
In: Burhenne, Wolfgang E., Perband, Klaus (Hg.): EDV-Recht. Loseblattsammlung

(115) Kevenhorster, Paul; Hoschka, Peter; Kalbhen, Uwe:
Informationslucke des Parlaments, Informationsprobleme der parlamentarischen Kontrollfunktion und Auswirkungen des DV-Einsatzes auf die Gewaltenteilung.
In: Hoschka, Peter; Malbhen, Uwe (Hg.): Datenverarbeitung in der politischen Planung.
Frankfurt, New York 1975, S. 233-256

(116) Knabben, Walter:
Die Haftung des Datenschutzbeauftragten aus unerlaubter Handlung und Moglichkeit der Haftungserleichterung gegenuber dem Geschaftsherrn.
In: Datenschutz-Berater (1977) H.6 S.84

(117) Kriependorf, P.:
Grundzuge der Subsidiaritat des Bundesdatenschutzgesetzes.
In: Datenschutz und Datensicherung (1977) H.2 S.66-69

(118) Kriependorff, Peter; Dummel, Hansjorg:
Datensicherung im Rechtssystem des BDSG.
In: Datenschutz und Datensicherung (1978) S.186

(119) Kroger, K.:
Der Datenschutz im Bereich der Offentlichen Verwaltung nach dem Bundesdatenschutzgesetz.
In: Die offentliche Verwaltung 30(1977) H.9 S.301-305

(120) Kroloff, G.:
The New World Information Order.
In: Data Regulation European and Third World Realities, Conf.Proc., S.195-206

(121) Langhorne, R.W.:
Trans National Data Regulations Impact on Private Enterprise.
Eurocomp' 78, London 1978

(122) Langhorne, R.W.:
Private enterprise concerns about data protection and transborder data regulations.
In: Data Regulation European and Third World Realities,Conf.Proc., In: Online Conferences (ed.): Uxbridge, 1978, pp. 135-157

(123) Layton, C.:
Protection of privacy - future prospects at the european communities level.
In: OECD, ICCP Vol.1,Paris 1979, S.213-216

(124) Lenk, Klaus:
Datenschutz in der offentlichen Verwaltung.
In: Kilian u.a. (Hg.): Datenschutz. Frankfurt 1973, S. 15 ff.

(125) Lindop, Norman:
International protection of personal data - reciprocity or harmonisation?.
In: OECD, ICCP Vol. 1,Paris 1979, S. 288-292

(126) Linowes, D.F.:
National privacy concerns in the United States of America.
In: Data Regulation European and Third World Realities, Conf.Proc., S. 93-104

(127) Longsworth, M.A.:
Transborder data flows and the protection of privacy - CBEMA's view.
In: OECD, ICCP Vol. 1, Paris 1979, S. 74-80

(128) Lutterbeck, Bernd:
Parlament und Information. Rechtstheorie und Informationsrecht 3.
Munchen/Wien 1977

(129) Lutterbeck, Bernd:
Erfahrunger des Bundesbeauftragten fur den Datenschutz bei Kontrollen im offentlichen Bereich - Vortrag anlablich des 16. Erfahrungsaustausches
ADV/Bund/Lander/kommunaler Bereich.
Mainz 1979

(130) Maennecke, Winfried:
Verwaltungsvorschriften der Landeraufsicht fur den Datenschutz.
In: Der Betrieb (1978) H.20 S.971

(131) Mallmann, O.:
Datenschutz in Schweden: Das neue Datenschutzgesetz.
In: Offentliche Verwaltung und Datenverarbeitung 4(1974) H.1 S.31-33

(132) Michel. J.:
L'impact des reseaux de transmission de donnees.
In: OECD, ICCP Vol. 1,Paris 1979, S. 144-146

(133) Ministry of Defense, Sweden:
The Vulnerability of the Computerized Society.
Stockholm 1978

(134) Norman, A.R.D.:
A scheme for regulating trans-border data flows.
In: Data Regulation European and Third World Realities, Conf.Proc., S. 122-134

(135) Norris. W.:
A businessman's perspektive on the transborder data flow issue.
In: Data Regulation European and Third World Realities, Conf. Proce., S. 1-12

(136) Nowak. R.:
Data protection in transborder data flows in the banking sector.
In: OECD, ICCP Vol. 1,Paris 1979, S. 124-126

(137) Onstad, P.C.:
Data processing services and transborder data flows.
In. OECD, ICCP Vol. 1,Paris 1979, S. 178-182

(138) Ordemann, Hans-Joachim:
Internationale Datenflusse - europaische Datenschutzkonvention
In: Computerwoche (1977) H.23 S.6

(139) Ordemann, Hans Joachim:
Grenzuberschreitender Datentransport - internationales Datenschutzubereinkommen.
In: Offentliche Verwaltung und Datenverarbeitung (1977) H.6 S.3-7

(140) Ordemann, Hans-Joachim; Schomerus, Rudolf:
Bundesdatenschutzgesetz mit Erlauterungen.
2. Aufl. Munchen 1978

(141) Osborn, J.L.:
Corporate employee information handling practices and employee perceptions.
In: OECD, ICCP Vol. 1,Paris 1979, D.261-266

(142) Parker, E.:
Social implications of computer/telecoms. systems.
In: Data Exchange (1978) H.3/4 S.3-13

(143) Parsons, C.:
The U.S. privacy protection study commission.
In: OECD, ICCP Vol. 1, Paris 1979, S.242-248

(144) Pipe, G.R.:
Transnational Data Regulation, Reviewing the Issues.
In: Transnational data regulation.
Proceedings Online conference Brussels 1978,
S. 233-240

(145) Pipe, G.R.:
An Assessment of Views on Transnational Data Regulation.
Conference paper, on-line-conference,
Brussels 1978

(146) Pipe, G.R.:
International organisations face the information communication revolution.
In: Data Regulltion European and Third World Realities, Conf.Proc., S.185-194

(147) Pipe. G.R.:
Comparison of Features of Current Data Protection Legislation.
In: Review Briefings Eurocomp 78, Online-conference, London 1978

(148) Pipkorn, Jorn:
Transnationale Perspektiven behordlicher Informationspflichten.
In: Die offentliche Verwaltung (1976) S.340

(149) Podlech, Adalbert:
Verfassungsrechtliche Probleme offentlicher Datenbanken.
In: Die offentliche Verwaltung 23(1970) S.473-475

(150) Podlech, Adalbert:
Vertfasungsrechtliche Probleme offentlicher Informationssysteme.
In: Datenverarbeitung im Recht Bd. 1(1972) H.2/3 S.149-169

(151) Podlech, Adalbert:
Prinzipien des Datenschutzes in der offentlichen Verwaltung.
In: Kilian, Wolfgant u.a. (Hg.): Datenschutz. Frankfurt 1973, S. 3 ff.

(152) Podlech, Adalbert:
Aufgaben und Problematik des Datenschutzes.
In: Datenverarbeitung im Recht Bd. 5(1976)
H.1/2 S.23-40.

(153) Privacy Protection Study Commission:
Personal Privacy in an Information Society.
The Report of the Privacy Protection Study
Commission.
Washington 1977
6 vol. incl. 5 append.

(154) Read, C.N.:
Banking and the regulation of data flows.
In: OECD, ICCP Vol. 1,Paris 1979, S.139-142

(155) Reh. Hans - Joachim:
Gegenstand und Aufgabe des Datenschutzes in
der offentlichen Verwaltung.
In: Beitrage zum Datenschutz (1974) H.2

(156) Richardson, J.M.:
Some observations about barriers and ease of
transborder data flow.
In: OECD, ICCP Vol. 1,Paris 1979, S.310-311

(157) Rodota, S.:
Legislation et la libre circulation de
l'information.
In: OECD, ICCP Vol. 1,Paris 1979, S.308-309

(158) Ruckriegel, Werner:
Richtlinien fur die Datenschutz-Aufsicht.
In: Der DSB-Kongreb '78, Dusseldorf, 8.-10. Mai 1978. Dokumentation, I PR 02

(159) Sasse, Christoph; Schweinoch, Joachim:
Bundesdatenschutzgesetz.
Stuttgart 1977
Loseblattkommentar

(160) Schaffland, Hans-Jurgen; Wiltfang, Noeme:
Bundesdatenschutzgesetz (BDSG). Erganzbarer Kommentar nebst einschlagigen Rechtsvorschriften.
Berlin 1977

(161) Schedl, Ilse:
Bundesdatenschutzgesetz.
Kissingen 1977

(162) Schindel, Jost:
Der amerikanische Datenschutz von 1974.
In: Beitrage zum Datenschutz (1975) H.3

(163) Schindel, Jost:
Das franzosische Datenschutzgesetz vom 6.1.78 - eine burgerfreundliche Regelung.
In: Datenverarbeitung in Steuer, Wirtschaft und Recht (1978) S.237

(164) Schimmel, Wolfgang; Steinmuller, Wilhelm:
Rechtspolitische Problemstellung des
Datenschutzes.
In: Dammann, Ulrich; Karhausen, Mark; Muller,
Paul; Steinmuller, Wilhelm: Datenbanken und
Datenschutz. Frankfurt /M 1974, 111

(165) Schimmel, Wolfgant:
Die institutionelle Kontrolle des
Datenschutzes nach den Datenschutzgesetzen
der Lander.
In: Datenschutz und Datensicherung (1979) H.1
S.25-30

(166) Schlanitz, E.:
Les flux de donnees transfrontieres dans le
contexte de la cooperation policiere
internationale.
In: OECD, ICCP VOL. 1,Paris 1979, S. 102-105

(167) Schomerus, R.:
Datenschutz in den Vereinigten Staaten.
In: Offentliche Verwaltung und
Datenverarbeitung (1977) H.11 S.3-7

(168) Schomerus, R.:
Das franzosische Datenschutzgesetz.
In: Datenschutz und Datensicherung (1978) H.2
S.61

(169) Schomerus, R.:
Regulation of Transfrontier Data Traffic
under the Federal data Protection Law.
In: Transnational data regulation.
Proceedings Online conference Brussels 1978,
S. 221-226

(170) Schomerus, R.:
The German Federal Data Protection Act.
In: Data Regulation European and Third World
Realities, Conf.Proc., S.85-92

(171) Schwappach, Jurgen:
Bundesdatenschutzgesetz mit Erlauterungen.
Bergisch-Gladbach 1977

(172) Schweinoch, Joachim:
Vorlaufige Verwaltungsvorschriften zum
Bundesdatenschutzgesetz.
In: Datenschutz und Datensicherung (1978)
S.119

(173) Schweinoch, Joachim:
Aufsichtsbehorden und allgemeine
Verwaltungsvorschriften zum BDSG.
In: Datenschutz und Datensicherung (1978) H.1
S.11

(174) Schwappach, Jurgen:
Internationale Datenflusse im Bereich der Industrie und ihre Bewertung nach dem Datenschutzgesetz.
In: Datenschutz und Datensicherung (1978) H.1 S.21

(175) Schwappach, J.:
International data flows in the industrial sector.
In: OECD, ICCP Vol. 1,Paris 1979, S.217-223

(176) Seipel, P.:
Computing Law.
Stockholm 1977

(177) Seligman, N.:
The importance of empirical research.
In: OECD, ICCP Vol. 1,Paris 1979, S.86-90

(178) Shickich, J.E.:
Transborder Data Flow.
In: Law and Computer technology (1978) H.3 S.62-74

(179) Sieghart, Paul:
Privacy and Computers.
London 1976

(180) Sieghart, P.:
The protection of personal data - lacuna and overlap.
In: OECD, ICCP Vol. 1,Paris 1979, S.224-230

(181) Simitis, Spiros:
Datenschutz - Notwendigkeit und Voraussetzungen einer gesetzlichen Regelung.
In: Datenverarbeitung im Richt Bd. 2(1973) H.2/3 S.138-189

(182) Simitis, Spiros:
Gesellschaftspolitische Implikationen juristischer Dokumentationssysteme.
In: Datenverarbeitung im Recht Bd. 3(1974) H.1/2 S.1-56

(183) Simitis, Spiros:
Bundesdatenschutzgesetz - Ende der Diskussion oder Neubeginn?.
In: Neue Juristische Wochenschrift 30(1977) S.729 ff.

(184) Simitis, Spiros; Damman, Ulrich; Mallmann, Otto; Reh, Hans Joachim:
Kommentar zum Bandesdatenschutzgesetz.
1. Aufl. Baden-Baden 1978

(185) Spieker, W.:
Data protection and the trade unions.
In: OECD, ICCP Vol. 1,Paris 1979, S.233-235

(186) Stadler, G.:
Datenschutz in der Human Rights Bill von Kanada.
In: Offentliche Verwaltung und Datenverarbeitung - Online - ADL-Nachrichten (1977) H.5 S.16

(187) Stadler, G.:
Grenzuberschreitender Datenverkehr und Datenschutz.
In: Online adl-Nachrichten (1977) H.11 S.923-924

(188) Stadler, Gerhard:
To International Regulations on Data Flows and Privacy Protection.
In: Transnational data regulation. Proceedings Online conference Brussels 1978, S. 95-112

(189) Stadler, G.:
Options for privacy protection in international data flows.
In: Data Regulation European and Third World Realities, Conf.Proc., S.37-58

(190) Stadler, G.:
From national to international legislation on information flow and data protection.
In: OECD, ICCP Vol. 1,Paris 1979, S.42-50

(191) Steinmuller, Wilhelm; Lutterbeck, Bernd; Mallmann, Christoph; Harbort, Ulrich; Kolb, G.; Schneider, Jochen:
Grundfragen des Datenschutzes. Gutachten im Auftrage des Bundesministeriums des Innern.
In: Bundestags-Drucksache VI/3826, Bonn 1972, S. 5 ff.

(192) Steinmuller, Wilhelm:
Datenschutz als Teilaspekt gesellschaftlicher Informationskontrolle
In: Deutsche Sektion der internationalen Juristen-Kommission (Hg.): Datenschutz und Datensicherung. Karlsruhe 1975, S. 35 ff.

(193) Stromberg, G.:
International message transfers between banks.
In: OECD, ICCP Vol. 1,Paris 1979, S.133-138

(194) Taib, A.:
Flux de donnees transfrontieres - aspects culturels et economiques.
In: OECD, ICCP Vol. 1,Paris 1979, S. 293-297

(195) Tourtellot, J.B.:
A World Information War?.
In: European Community Information
Service, (1978), Jan./Feb., S. 11 ff.

(196) Treille, J.M.:
L'information economique et industrielle: ses
sources et ses canaux de distribution.
In: OECD, ICCP Vol. 1,Paris 1979, S.160-165

(197) Tuner, Lotte;
Personlichkeitsrecht und Datenverarbeitung -
Die Weiterentwicklung des Datenschutzes durch
die Landesgesetzgebung.
In: Die neue Ordnung 32 (1978) H.2

(198) Tuner, Lotte;
Vorschriften zur Wahrung des Gleichgewichts
der Gewalten in Datenschutzgesetzen und
-entwurfen der Lander.
In: Datenverarbeitung in Steuer, Wirtschaft
und Recht 8(1979) H.4 S.89-94

(199) Turn, Rein:
Implications of Privacy Protection in
Databank Systems.
In: Database Journal of the ACM, 1975. S. 3-9

(200) Turn, Rein:
La securite des donnees: couts et
constraintes.
In: Prganisation de cooperation et de
development economique, OCDE etudes
d'informatique no. 10, Paris 1976, S.276-302

(201) Turn, R.:
Implementation of Privacy and Security
Requirements in Trans-National Data
Processing Systems.
In: Transnational data regulation.
Proceedings Online conference Brussels 1978,
S. 113-132

(202) Vandenberghe, H.:
La vie privee et les banques de donnees.
In: OECD, ICCP Vol. 1,Paris 1979, S.249-256

(203) Vinge, P.G.:
Experiences of the Swedish Data Act.
Stockholm 1975

(204) Walker, P.M.:
Barriers to Achieving the Full Potential of
International Data Communications.
In: Transnational data regulation.
Proceedings Online conference Brüssels 1978,
S. 181-188

(205) Wittkamper, Gerhard:
Datenschutz im Verpflechtungsbereich von staatlichen und ausserstaatlichen Bereich.
In: Datenschutz und Datensicherung (1977) H.1 S.12

(206) Wittkamper, G.W.:
Datenoasen - ein Mythologem?.
In: Datenschutz und Datensicherung (1978) H.2 S.59-60