

<b>GMD</b>	<b>IRIA</b>	<b>NCC</b>

**STUDY ON**

**DATA SECURITY AND  
CONFIDENTIALITY**

**SUMMARY REPORT**

**to the Commission of the European Communities**

**MARCH 1980**

<b>GMD</b>	<b>IRIA</b>	<b>NCC</b>

**STUDY ON**

**DATA SECURITY AND  
CONFIDENTIALITY**

**SUMMARY REPORT**

**to the Commission of the European Communities**

**MARCH 1980**

## Contents of full report

<b>Volume 1</b>	<b>Section 0:</b>	<b>Introduction</b>
	<b>Section 1:</b>	<b>Quality and quantity of transborder data flows, by J-P Chamoux, A Grissonnanche</b>
<b>Volume 2</b>	<b>Section 2:</b>	<b>Organization and method of operation of the data protection authorities, by H Burkert</b>
<b>Volume 3</b>	<b>Section 3:</b>	<b>The physical person/non-physical person problem, by F Bancilhon, J-P Chamoux, A Grissonnanche, L Joinet (counsellor)</b>
<b>Volume 4</b>	<b>Section 4:</b>	<b>International economic aspects of data protection, by E F M Hogrefe</b>
<b>Volume 5</b>	<b>Section 5:</b>	<b>Technical aspects of the right of access, by F Bancilhon, L Joinet (counsellor)</b>
<b>Volume 6</b>	<b>Section 6:</b>	<b>Data protection inspection, by H H W Pitcher</b>
	<b>Section 7:</b>	<b>Conclusion</b>

CONTENTS OF THIS SUMMARY REPORT

page number

0	Introduction	3
1	Quality and quantity of transborder data flows	9
2	Organization and method of operation of the data protection authorities	14
3	The physical person/non-physical person problem	24
4	International economic aspects of data protection	27
5	Technical aspects of the right of access	38
6	Data protection inspection	43
7	Conclusion	50
	Complete contents list of section 1	63
	Complete contents list of section 2	65
	Complete contents list of section 3	67
	Complete contents list of section 4	68
	Complete contents list of section 5	73
	Complete contents list of section 6	74



## 0 Introduction

### 0.1 Origin of this project

On 27 September 1977 the Council of Ministers of the Commission of the European Communities decided (decision number 77/616/EEC) to initiate three joint studies in informatics. The first of these, on data security and confidentiality, was described as follows:

The main object of this study is to examine, in conjunction with the Committee of National Experts convened by the Commission, the chief problems relating to the harmonization of Community legislation covering the protection of private life and the development of codes of application and corresponding standards.

The work will include analysis and classification of the problems and, in particular:

- estimates of the quantitative and qualitative aspects of the movement of data across frontiers inside and outside the Community,
- possible role of Community standards with a view to easier control of such movement, reduction of costs and opening of markets as a complement to effects of legislation - identification of priorities for the adoption of Community standards,

- preparatory studies with regard to cost estimates.  
Costs and possible distortion of competition which could ensue from different national legislations; costs resulting from Community harmonization; impact of costs borne by the public and private sectors and by individuals,
- identification of appropriate measures offering equivalent security at Community level,
- analysis of studies undertaken at national level in the Member States and other countries such as Sweden and the United States,
- analysis of problems relating to data security which could have an effect on confidentiality, legislation and standards, and a definition of the studies which should be carried out.

The continuation of work resulting from this analysis will be decided upon in the context of the multiannual programme.

Following this decision, three objectives were identified:

1. examining the need for harmonization of legislation, recommendations and standards on privacy;
2. improved control of computer data security including its technical feasibility and financial implications;

3. improved insight into the impact of privacy and security measures.

In view of these, six items were selected by the Steering Committee consisting of delegates from the three institutes (GMD, IRIA, NCC), in close consultation with the Committee of National Experts:

1. Quality and quantity of transborder data flow.
2. The character of the organization and the technical practice of Data Inspection Boards.
3. The natural person/other legal entity problem.
4. International economic aspects of data privacy regulation.
5. Technical aspects of the right of access.
6. Control, audit and enforcement of privacy requirements and their impact on security.

These items did not cover the whole area of the subject, but were considered to have priority because of their urgency, importance and general interest; the Council had foreseen that further work would be needed in the multiannual programme.



## 0.2 Motivation for the items in the study

The first item, on transborder data flows, is explicitly mentioned in the Council's decision. The possibility of frustration of data protection by processing personal data outside controlled areas, the distortion of competition which could result from this, and unease which had already been publicly expressed reinforce its topicality.

The second item, on data inspection boards, seeks to shed light on one aspect of data protection legislation which has been treated differently in different countries. Any attempt at harmonization of legislation will need to take into account not only the rules defining the powers and duties of such boards, but also their administrative practices.

The third item, on the natural/legal person question, relates to a topic which has been treated differently in the laws of different countries, and which has been the subject of international controversy.

The fourth item, on the cost aspect, is seen as an important practical matter about which further information is needed. In particular, the cost of complying with different, and possibly conflicting, national laws, and fears that international trade both inside and outside the EEC will be distorted by such differences, motivated the inclusion of this item.

The fifth item, on the right of access, relates to one of the central requirements of any data protection law. The possibility of efficient and economical satisfaction of this obligation, without prejudice to security and other aspects of data protection, and without undue interference in the legitimate work of the data user, is of interest to all involved in the subject.

The sixth item, on data protection inspection, is concerned with the problem of ensuring that data protection laws are observed; some measures in this area are considered necessary, and it is hoped that procedures can be defined which are useful in different countries and which will give confidence to the public that their interests are indeed safeguarded.

Although all three institutes bear responsibility for all six items, prime responsibility for each item was assigned to one institute as below, with the stated approximate manpower:

item 1	IRIA	3 manmonths
item 2	GMD	3 manmonths
item 3	IRIA	4 manmonths
item 4	GMD	6 manmonths
item 5	IRIA	4 manmonths
item 6	NCC	10 manmonths

The following are those who did most of the work in this study:

for GMD: H Burkert, E F M Hoglebe

for IRIA: F Bancilhon, J-P Chamoux, A Grissonnanche

for NCC: H H W Pitcher

The project leader for the Commission was Emile Peeters. This English version of the final report was produced at NCC.

### 0.3 Structure of the summary report

After this introduction, each item is treated separately in the corresponding sections numbered 1 to 6; the final section 7 describes the main features of the collaboration of the institutes in this work, and gives suggestions of topics deserving further study.

## 1 Quality and quantity of transborder data flows

This study has assembled information on the current state of transborder data flow (TBDF) within the European Economic Community and between member states and outside countries. This information falls under three headings:

- major data flows at present
- classification of these flows
- quantification of these flows.

The major dataflows at present have been analysed following a survey which revealed their great diversity, as much with respect to the character of the operators of these flows as to the nature of the transmitted data and the medium used. These TBDFs did not originate with computing: the need for them, and their existence, result from the freeing of trade and from its new world-wide scale, which require businessmen and information to travel more and more throughout Europe and the world. Nevertheless, the computerisation of companies, now just at its beginning, will result in increasing quantities of transmitted information and higher transmission speeds. So we can foresee in the next few years a large increase in the amount of TBDF because of the spreading business use of computers.

We must note that this computerisation at present concerns only companies, so the only existing flows are

professional ones. But private TBDF will appear in the next few years, resulting from the integration of computers in everyday life. Electronic mail is an example of such private development of computers; some of our air-mail letters will become electronic TBDF.

Besides these traditional flows, computing has created specific flows of a new kind: exchanges of programs, transfers of raw data and of information about data processing, computer bureau services, etc. But the amount of this new part of TBDF seems to be very small at present, representing only a few percent of the total as revealed by our enquiry.

The classification of TBDF which we have presented emphasises the basic dichotomy between:

- dataflows using a material medium: magnetic tapes, discs, punched cards, etc.
- dataflows using telecommunications.

This distinction seems unquestionable. Even if the actual data carried by post and telecommunications are of the same nature, the flows differ in their status as regards customs, postal, telecommunications, trade and tax regulations. Further, the structure of costs is different in each case. This distinction, though it is necessary, does not cover all the needs of analysis, and we saw that other criteria must be used to make an orderly census of TBDF:

- the distinction between personal data and non-personal data and, within personal data, between data about a physical person and data about a non-physical person
- the distinction between commercial flows and non-commercial flows
- the operator's character
- the direction of the exchanges, especially when countries outside the European Community are involved, and in particular USA.

As regards the quantification of TBDF, our survey pointed out the difficulty of obtaining useful information by direct enquiry. Systematic statistical data on this subject at a national level seems to be lacking. On the other hand, it turned out to be very difficult to get information from sources such as companies. The large number of information sources would require the setting up of a very powerful means of enquiry, out of proportion to this initial study. Further, this kind of data is generally considered confidential by companies, which would obviously hamper its collection, even for a statistical survey.

Lastly, from a theoretical point of view, a substantial effort is still needed to define more precisely a satisfactory method of evaluation of TBDFs. The ideas on this subject presented in 1.3.4 could constitute the starting-point of more extensive research in the continuing Community programme.

In conclusion, this study emphasizes the importance of TBDF for European countries. This has three aspects:

- a) A commercial stake: we have pointed out how much TBDF is bound up with the internationalisation of the western economy and with its liberal character. In some sectors of the economy (banks, financial institutions, airlines, and all multinational companies) the maintenance and development of free exchanges of information, and the possibility of using for them the most suitable medium, as regards cost, quantity and speed of communication, remains fundamental. Therefore we must watch over the maintenance and development of such exchanges in Europe, while respecting the principles of individual freedom and free competition established in the European Community's treaties.
  
- b) A cultural stake: we have pointed out in this section how great is the risk of cultural alienation. The risk comes from the development of new information media, such as those now required for the press. The development of such new technologies must not help the creation of monopolies benefiting only companies outside the European Community. Third-world countries are by now quite conscious of the problems of an American-dominated press, and attach great importance to achieving a better balance in this field. Among developed countries also, this balance

must be maintained. Concerning databanks, the Euronet network is an important factor, which should allow Europe to take up a challenge posed by the American databanks and information retrieval systems which have established their reputation.

- c) An industrial stake: the connection of data processing and telecommunications will give rise to a wide range of new products and services. Many have already embarked on this course in Europe. The entry of IBM in such a project as SBS clearly shows how attractive the future seems for large companies combining data processing and telecommunications. But it also clearly shows that it will become more and more difficult to sell data processing equipment without integrating it in large networks. Information competition will demand, in this field too, that European companies give themselves world-wide range and equal opportunity to the largest American trusts.



## 2 Organization and method of operation of the data protection authorities

### 2.0 Relevance of the item and approach

Any discussion of a possible harmonisation of data protection in the EEC has to consider the legal material already developed in that area. Even more important, however, is the way in which data protection legislation is or is intended to be implemented. Main agencies of this implementation are the data protection authorities.

We have therefore described these authorities in the EEC area and we have also included Sweden because of its outstanding experience. The description is mainly based on the drafted or enacted data protection laws (deadline 1 September 1979), but also includes experiences and methods of operation (especially licensing procedures and inspection methods - see also section 6 of the final report).

On the basis of this material we have come to some general but preliminary conclusions on the role and significance of these institutions. From these conclusions we have then derived some suggestions with regard to the future importance of these agencies, especially vis-à-vis the recent recommendations of the European Parliament.

## 2.1 Data protection agencies in the context of national data protection laws and draft laws in the European Economic Community and Sweden

In the final report (section 2.1) we have described the data protection authorities of Denmark, France and Luxemburg in the framework of the existing laws, and the envisaged control authorities of Belgium, the United Kingdom and the Netherlands (on the basis of the most frequently discussed drafts and reports). The data protection systems of the Federal Republic of Germany and Sweden have received a more detailed description (in section 2.2 of the final report), since more experience was available there at the time of the report. In detail (country: main legal source document/institution described):

Belgium: Draft: Vanderpoorten (1976)/Commission d'Inspection

Denmark: Private Registers etc. Act (1978), Public Authorities Registers Act (1978)/Data Surveillance Authority

France: Loi no. 78-17 du 6 janvier 1978 relatif à l'informatique, aux fichiers et aux libertés/Commission Nationale de l'Informatique et des Libertés

United Kingdom: Lindop Report (1978)/Data Protection Authority

Luxemburg: Loi du 31 mars 1979 reglementant l'utilisation des donnees nominatives dans les traitement informatiques/Ministre competent and Commission Consultative

Netherlands: Draft Bill on Personal Data Systems (1976)/Registration Board

Federal Republic of Germany:

On the federal level: Gesetz zum Schutz vor Missbrauch personenbezogener Daten bei der Datenverarbeitung (1978)/Federal Commissioner for Data Protection (public sector, federal level) and Supervisory Authorities (private sector)

On the Land level: Hessisches Datenschutzgesetz (1978) (as an example for the public sector, Land level)/The Hesse Data Protection Commissioner

Sweden: Data Act (including the modifications of 1 July 1979)/Data Inspection Board

For each of these, we have described, as of interest to the user, the conditions under which data processing is permitted (with emphasis on the private sector). As of interest to the data subjects, we have outlined the rights they can exercise and the conditions under which

they can exercise them. Having thus characterised the field of operation of the data protection authorities, we have then specified their structures, tasks and method of operation. Special emphasis was given to the institutions of Germany and Sweden since they already had implementation experience.

We think it worthwhile, as soon as more experience is available, to make also secondary material such as application forms, regulations and directives accessible on an EEC level, and to give a manual (to be updated regularly) to users and other interested parties who wish to operate within the EEC.

We have refrained from classifying data protection authorities to avoid any misleading oversimplifications that tend to arise with such summary surveys. It has been our main intention with these descriptions to show that the specific national solutions of the problems of data protection are closely connected to the political and legal tradition of each country.

On the other hand, we have realised some general trends with regard to these authorities, which arise from the fact that the problems of data protection present themselves in the EEC and in Sweden in a very similar way.

## 2.2 Role and significance of the data protection authorities

These general observations have been presented in section 2.3 of the final report as a first attempt to judge the role and significance of these authorities both on national and international level.

We have identified the data protection authorities as unique types of administration even within their own national environment. As the main feature of this new type, we have pointed out the dialogue-orientated form of operation which leads to specific demands on the staff and administrative structure.

This feature results from the specific function this kind of organisation has to fulfil: although they act as control agencies, they operate in a preventive rather than in a repressive manner and put high emphasis on education, at least at the present stage. They thus help to provide general acceptance for information technologies in modern societies.

On the international level, they have to observe the area of transborder data flow in order to counterbalance international developments that might weaken the national acceptance of data protection. So their main criterion, when they give opinions or decisions in that area, is whether the level of data protection achieved nationally is guaranteed abroad. At the same time, within their

educative functions, they have to give assistance to users and persons concerned in questions of transborder data flow. In this area we have observed already well operating forms of international co-operation, a development that dates back to the phase of "emerging data protection in Europe", when these agencies gave each other assistance in their planning stages.

This picture, however, represents only an impression of the situation at the time when this report was drafted. With the recommendation of the European Parliament and its accompanying report, new demands have been put forward to these authorities, to national legislators in the EEC and the Commission.

### 2.3 Future demands on the data protection authorities within the EEC

These demands and future trends in the development of data protection authorities have been analysed in section 2.4 of the final report.

On the basis of this preliminary study, we have come to the following conclusions with regard to the recent recommendations of the European Parliament:

Each of the laws and drafts analysed provides for some kind of data protection agency. Though their powers differ widely, each organisation includes a publicly accessible register, which, however, also differs in its extent. Nevertheless these organisations already represent the nucleus of a practicable international co-operation that can take care of the specific demands within the EEC.

Further demands on these authorities (with regard to harmonising their decision-making and/or licensing powers) should, at the present stage, be left for the individual nations to develop, since some of these agencies have not even been implemented, while others are still in their consolidation phase. Any outside attempt to impose new structures or jurisdictions - at least at the present stage - might endanger their role of encouraging national acceptance of information technologies and hinder their effectiveness.

With regard to transborder data flow, it is difficult to foresee that countries already having a high national level of data protection would leave that in favour of a lower but more generally accepted level. International agreements or harmonisation procedures that do not leave the option of restricting transborder data flow in specific cases are likely to fail.

This is especially so, because the above-described role and functions tend to lead to a stronger political involvement of these authorities, whether intended or not. They have to provide acceptance for a technology that has become enormously important to the national economy, internal and external security and national sovereignty. At the same time, these agencies represent a high concentration of expertise and factual knowledge in that field. This stronger political involvement can be seen in the fact that, though initially questions of data protection were more or less all-party issues, the modification of existing laws and the development of sectoral data protection (internal security, social security, employer/employee relationships) have become controversial issues. In the field of transborder data flow, issues of national economy and sovereignty become increasingly intermingled with the original data protection issue.

This development must be closely watched, outside the EEC as well, and any artificial restriction to that area is likely to be impractical.

Instead, it is suggested that in the field of international data protection law, an upward approach should be attempted, i.e. national legislation and EEC activities should give whatever assistance they can to the practical co-operation of existing and upcoming data protection authorities, including those outside the EEC.



Only on the basis of day-to-day co-operation, as already in practice between existing agencies, can long-range workable solutions be developed in this complex area.

#### 2.4 Possible keypoints for future research

Our awareness of the complexity of the data protection issue, seen nationally in the discussions on the modification of existing laws and the implementation of sectoral data protection, and internationally in the attempts to draft international agreements, leads us to stress the necessity of further joint scientific observation and research in this area (see section 2.5 of the final report).

Within the area of research already covered by this study we suggest:

- further compilation and analysis of secondary legal material, i.e. decisions of the data protection authorities, sectoral regulations, forms, etc., issued by the relevant authorities, possibly compiled in a periodically updated user handbook;

- analysis of decisions and regulations in the area of transborder data flow, with special consideration of issues that are not prima facie issues of data protection.

Outside the area of the present research we suggest:

- inclusion of the third-world countries in the above-mentioned research, with special emphasis on consequences that affect the EEC as such;
- analysis of the role of a possible future EEC Data Protection Body, taking into account the suggested upward approach;
- consequences in the area of sectoral data protection, especially the protection of research data in the EEC;
- possible educative measures in the area of data protection both for the user and data subject in the EEC.

### 3 The physical person/non-physical person problem

Due to the superficial reactions of the general public, which were gauged during the recent conference in Paris on 'Data Processing and Society', it is becoming a generally accepted social objective to ensure that a European citizen has a satisfactory awareness of the places where he is on file, and the information contained in these files. By a strange accident of history, the idea of giving non-physical persons protection of the same type as that which is offered today to physical persons has asserted itself more and more. Having been rejected by the German and French parliaments, this extension of protection to non-physical persons gradually asserted itself in the most recent laws, in Denmark, Luxemburg and Norway.

We show, in this report, that the extension of the computing laws gives rise to two large problems: a conceptual problem, that of defining protection of non-physical persons in terms of principles, and the problem of interpretation in limiting the field of application of protection of physical persons when these persons are not mentioned by name in the files.

The first problem has not been solved in a satisfactory manner by the laws currently passed by the member countries. We have suggested that it should be considered as a commercial right, and not as a human

right as in the majority of current laws. If one admits that non-physical persons, and particularly commercial agents, have a legal interest in keeping a strict control on information which they hold, a control which is ruled by the customary right of business secrecy, the concept of privacy in the strict sense can apply only to human beings, and not to companies or associations. Thus it seems desirable to specify a purely commercial doctrine of secrecy and disclosure of data which concerns commercial activity, and particularly that of commercial non-physical persons, in order to avoid in future permanent confusion between similar but distinct concepts, which one sometimes wrongly treats as one. If such a doctrine developed, and if it could be operated in Europe, it is probable that one could assimilate it to the principles of the Treaty of Rome regarding fair competition (articles 85-86).

The second problem is relatively easier to resolve. Whenever connections between physical and non-physical persons are implicit in the choice of the information recorded on file, it is probable that the laws should apply as if the file referred only to physical persons. Anyway, one should beware of a gradual extension of the field of application of the laws which would eventually take away their purpose.

Thus, it is necessary that future developments of the laws on files are based on a thorough analysis of the

need for protection of data, and the form of this protection for non-physical persons. Particularly one should distinguish between commercial companies and private associations, and also consider separately what protection should be given to companies in the public sector.

Thus we say in this report that future research should be directed towards a very detailed analysis of the need for protection and the means of applying it, especially as these needs should be based, in our view, on the Common Market's economic principles: balance of competition, and equity in commercial relationships. If this should develop, one could then imagine that the final objective of data protection in Europe would be based on two complementary principles: the protection of man and the citizen on the one hand, particularly with regard to files of physical persons; the protection of 'commercial' man on the other hand, in what concerns the non-physical person.

This is without doubt the common objective. But the means of access, of control, and of enquiry will doubtless be different for physical and non-physical persons. Today one is well aware of the means which apply to files of physical persons. Several years more will doubtless be needed before the same is true for the files of non-physical persons.

#### 4 International economic aspects of data protection

4.1 It was the task of section 4 to evaluate - as far as this is possible in a general way - the cost of data protection on a national level, and the possibly ensuing international distortion of competition. Furthermore, appropriate harmonising measures were to be identified which could reduce the cost of data protection, and in particular the possibly ensuing international distortion of competition; the rights and interests of the citizens concerned were to be taken into account especially.

In order to clarify the scope of the study, it has to be stated that section 4 concentrates on the one hand essentially on the cost of data protection in the sense of the costs which occur because of additional data protection measures. General inefficiencies or opportunity costs caused by data protection could not be dealt with in detail within the given framework. As far as the issue of international distortion of competition is concerned, it has to be stressed on the other hand that distortions of competition were to be discussed only where they are caused specifically by the cost of data protection, as opposed to those which might be caused by data protection in general.

4.2 After a general overview in section 4.1, section 4.2 examines certain basic concepts of economic theory in their relation to the data protection issue. These serve the theoretical evaluation and interpretation of the data protection cost issue and present suggestions and starting-points for possible follow-up studies. Moreover, certain theoretical and methodological difficulties in the evaluation of costs and benefits of data protection are dealt with, and the general theoretical concept and the concrete methodological approach of section 4 are explained.

In view of the inadequacy and unreliability of the available data, section 4 refrains almost completely from making quantitative statements, and concentrates on qualitative arguments and results on the basis of figures provided by various sources.

4.3 In section 4.3, various representative estimates, studies, and experiences from different countries relating to the cost of data protection are critically reviewed and evaluated. The following studies or experiences are dealt with in some detail:

- Great Britain (4.3.1): the Report of the Committee on Data Protection and the underlying PACTEL cost study

- USA (4.3.2): the Goldstein privacy cost estimation model, and the cost survey of the Office of Management and Budget (OMB)
- Sweden (4.3.3): the experience of the Data Inspection Board (DIB) with the Swedish Data Act
- Federal Republic of Germany (4.3.4): experience with the Federal Data Protection Act.

4.4 The general result of the evaluation of the various national estimates and experiences are summarised in section 4.4. In this context the unreliability of the existing - in particular quantitative - data protection estimates, and the ensuing - in tendency very considerable - overestimation of (genuine) data protection costs, constitute the main finding of the study. This holds basically for the overall data protection costs and for the individual data protection items, in particular for notification, access, data protection personnel, registration and licensing, data security, and opportunity costs.

The discrepancy between these findings and the various - in part extremely high - data protection cost estimates can be explained partly by the interests involved as far as certain comments from private industry are concerned, and partly by otherwise-motivated overestimates of data



protection costs as they occur in reality (e.g. for notification and access). Yet above all, cost-reducing factors are not taken into account adequately, and on the other hand various cost evaluations (or rather estimates) charge the costs of various measures - especially in the security area - incorrectly and in violation of the principle of causality to data protection, when these measures are taken - at least partly - on account of other obligations and requirements, and particularly out of the self-interests of the data processing body: in cost accounting, it would not be correct to consider these as data protection measures.

Moreover, the genuine data protection costs, which under application of correct principles of cost accounting are already rather insignificant, are, in the context of an overall evaluation of the charges which data protection puts on the personal data processing organisations, to be further reduced by various economies and other benefits of data protection. Therefore the thus-defined net charge put on data processing organisations by data protection appears in the end to be generally really marginal.

4.5 On the basis of these considerations concerning the data protection cost issue, section 4.5 deals with the issue of international distortion of competition caused by data protection costs. However, as already explained, data protection costs are generally speaking almost negligible, and in any case too small to have a substantial effect on the competitive strength of industry. In exceptional cases this assessment may possibly not be valid to the same extent, but this does not influence the overall judgement.

Therefore, the general conclusion can be drawn, that data protection costs are so small that they cause no international distortion of competition. Nor do certain relatively insignificant additional charges, which internationally operating companies (and multinational companies in particular) might incur because they have to cope with various differing national data protection regulations, add up to substantial effects of distortion of competition due to data protection costs. In particular, in comparison with other much more important international cost differences (e.g. in telecommunications tariffs), possible international data protection cost differences appear negligible.

4.6 With the exception of possible differences in access fees, the individual data subject is generally not harmed economically by differences between the various national data protection regulations, either.

Yet it has to be recognised that the individual is much more hampered, and in practice to a large extent even prevented, from exercising his data protection rights on an international level, than is the case for internationally operating companies with various international bases and representations. This, however, is not really a cost issue but a factual difficulty which obviously has certain economic implications (cost of legal advice on international data protection, translation, communication costs etc.) as soon as the person concerned tries seriously to overcome these difficulties.

4.7 In conclusion, section 4.6 lists various elements of European data protection harmonisation which would be favourable for the citizen and cost-effective at the same time. The basic reasoning is that, although a European data protection harmonising policy does not need to concentrate on reducing data protection costs and the corresponding distortion of competition (because the data protection costs are generally negligible, and

consequently the international distortion of competition of no practical relevance), the active and uniform realisation of the legitimate data protection objectives on an international level has to be striven for with the greatest possible efficiency.

In particular, in the realisation of the ambitious concept of the European Parliament for a directive on the harmonisation of legislation on data protection to provide citizens of the Community with the maximum protection, the following principles must be taken into account for reasons of efficiency: uniformity, simplicity, stability, predictability and the granting of adequate intervals for transition and adaptation.

The introduction on a European level of a basically uniform obligation to register and licence personal data files or applications seems to be equally important in the long run. Moreover, the introduction of a national data protection authority in each country appears on the one hand to be the logical complement to a registration and licensing scheme, and on the other hand to be necessary for the efficient implementation of national data protection regulations and international harmonising directives.

In particular on an international level, the individual should enjoy broadened notification and access rights (as far as possible free of charge), especially in order to

reduce the financial and other difficulties the individual encounters in exercising his data protection rights. The issue of strict data protection liability should also be dealt with uniformly on a European level, and favourably for the citizen.

4.8 At present, it is impossible to evaluate even approximately the cost of European data protection harmonisation. However, such costs should presumably not be a major issue if harmonisation is realised roughly on the lines discussed above.

4.9 Finally, section 4.7 identifies possible subjects for future economically oriented data protection research. The following issues appear specifically to need further investigation as a basis for the elaboration of European data protection directives:

- practical implications and costs of the public data protection supervisory authorities (European Community, Scandinavia, Austria, Canada), and estimation of the corresponding implications and costs of European data protection harmonisation (including financing schemes)

- elaboration of a body of European data protection statistics covering on a coherent basis the practical implications and costs etc. due to the various national data protection regulations (private sector)
- practical economic implications (cost etc.) of international data protection regulations in specific sectors of industry (address vendors/direct mail, banking and insurance, credit reporting etc., computer bureaux and data bank vendors etc.) with special regard to American sectoral data protection regulations
- study of the harmonisation issue on the level of state data protection regulations within and between the USA and Canada (with special regard to economic aspects)
- the issue of de facto distortions of international competition due to data protection
- practical implications and problems of international data protection regulations with regard to internal communications of multinational companies and groups (particularly in the areas of clients, marketing, financial and personnel data)
- function of data protection as an integral part of efficient data resource management at company level
- experience regarding the practical implications and costs of various international Freedom of Information regulations (Sweden, USA, Canada etc.)
- practical and economic aspects of the data protection issue with regard to new electronic information and communication technologies

- data protection, personal profiles, automatic decision-making, administrative and technical control technologies.

Apart from economic research parallel to the elaboration and implementation of European data protection directives, and the study of economic aspects of the legal person data protection issue, it is above all the general policy issue of the legal framework of a future European common data and information market which is of decisive importance. In view of the European infrastructure which is currently being put up in the data network and data bank area, and the European information industry evolving on this basis, the following specific research items are proposed:

- data and information liability or guarantee with respect to permanent availability, quality etc. of data banks services etc.
- proprietary rights with respect to electronic data and information, as well as services and products based on these
- rights of access and use by individuals and organisations of data banks, data networks, applications software, interpretational knowhow etc.
- private or public organisation of infrastructures in the area of information technology, information, resources, information industries etc.

- legal issues of authentication and evidence with respect to electronic data etc.
- private or governmental rights of access and inspection with respect to data banks etc. (e.g. as legal evidence, checking of data and interpretative or decision-assisting programs, publication of cryptographic transmission codes etc.).



## 5 Technical aspects of the right of access

In most data privacy laws one can find two distinct and almost contradictory aspects: the first one deals with the right of secrecy, the second with the right of knowledge. The right of secrecy consists in preventing an excessive divulgation of information concerning private individuals. The right of knowledge consists in giving a private individual free access to the information about himself that is stored by a third person.

From the very beginning of EDP, technical means were developed that helped to enforce the right of secrecy (data security, protection systems, encryption, etc.). Even though these means were not developed for this specific purpose, they are now available for the enforcement of this aspect of legislation. But no technical tools have been developed for the right of knowledge. In this study, we try to understand the technical implications of this right.

Since this study is concerned with the impact of legislation on technical developments, it is necessary to start by a better understanding of the technical state of the art. We therefore present a brief overview of future evolution in the computer field. We divide this field in three parts: information storage, information processing and information communication, and describe successively

the hardware and software evolution in these three areas: large public networks, local networks, mass storage (traditional technology, new technology, digital videodisc, database machines), software engineering, word processing and the general standardization effort. The conclusion of this brief survey is that (1) more data will be stored, (2) the structure of this data will grow more and more complex.

Having defined the technological perspective of our study, we then move to describe more precisely the right of access. We decompose this right into four parts:

Right 1: The right of the public to be aware of the existence of all files.

Right 2: The right of the individual to be aware of the existence of information held on him in a given file.

Right 3: The right of an individual to know the content of the information concerning him in a given file.

Right 4: The right of an individual to ask for the correction of data concerning him whenever necessary.

Then we study the actual implementation of each of these rights.

Right 1: We show that individual notification is not an adequate solution. Then we explain that different solutions can be envisaged, and that they are characterized by:

- (i) the number of information centres (is there a central one or several distribution points?)
- (ii) the types of information centres (is there just one type or are they organized by sector?)
- (iii) the information storage medium and the means of access to that information
- (iv) and last but not least, the content of that information.

Instead of choosing one optimal solution, we give a number of elements that must be taken into consideration for this choice, and we study the implication of each of these.

Right 2: After showing that this right is distinct from right 1, we distinguish two different approaches to a solution: the notification method and the information centre method.

We study the different problems in the notification method: periodicity of notification; the confidentiality problem due to the large flow of data generated by this

method. We also study in detail "implicit notification" and show its scope and limits.

The information centre method is then studied, together with the confidentiality problems that it generates.

Right 3: In this case again, two different approaches can be distinguished: the query method (the data subject asks the responsible keeper) and the notification method (the responsible keeper voluntarily notifies the data subject). In fact these two methods differ only in the first phase (query initiation), after which they have a common phase in which the system owner must communicate the information to the data subject.

Therefore we first study the query initiation process and show that it is closely related to the enforcement of right 1: the more precise the system description, the more precise will the query formulation be.

We decompose the process for answering the data subject's query into three steps: (1) defining the information relating to the data subject, (2) retrieving that information, (3) communicating it. In order to give a full description of the problems raised by these three steps, we first outline the various components of an information system. We show that information in such a system can exist in three forms: the basic data (the files themselves), the auxiliary data (for security and performance purposes), the application programs.

Right 4: We briefly describe this right, which is not an essential part of the right of access but a natural consequence. We show that a major problem is that of correction propagation, because of its cost and its possible threat to data confidentiality.

## 6 Data protection inspection

### 6.1 Purpose and form of the inspection

Much has been written about data protection laws, but little about how they could be enforced. Indeed, people have said that it would be easy to evade such laws without being caught, and therefore that they are bound to be ineffective.

The present study has been concerned with the means of checking whether a system which uses personal data complies with a data protection law. Such a means would not only help enforce the law: it could also tell the conscientious data user if and where his system needed improvement. It would thus support the law in a practical positive way, and give confidence to the public that their interests were safeguarded.

The envisaged form of the inspection is this in outline: A decision is made to inspect a particular system. (If it is a statutory inspection in pursuit of the law, this decision may be made by a Data Protection Authority; but an organisation may decide on a voluntary inspection of one of its own data systems.) An inspector (possibly more than one person) is appointed. He collects information about the system which is to be checked, mostly during a visit to the place where it is operated.

He interviews the people who are responsible for and operate the system, and examines different parts of it. He writes a report presenting his conclusions on the compliance of the system with the data protection law.

## 6.2 Adaptability of the inspection procedure

Different data protection laws and proposed laws contain a great variety of legal requirements. It might appear that an inspection procedure must be directly related to the particular law, compliance with which is being checked.

Similarly, systems using personal data are very various in size, complexity, mode of operation, and in the sensitivity of the data they contain.

Another factor which must affect the inspection procedure is the thoroughness which is required. Perhaps most systems do not pose a great threat to their data subjects; for these, a fairly superficial and economical check may be appropriate. But there are systems which, because of their size, the sensitivity of the data they contain, the concentration of power which they represent, or the public concern which they attract, justify a searching and unlimited investigation.

If each of these factors (as well as the statutory/voluntary possibility mentioned in the previous section) required different inspection procedures, the whole subject would be

complicated. It turns out that this is not so: the proposed inspection procedure can accommodate all data protection requirements, suit any data system, and be as exhaustive or superficial as circumstances require. Different parts of the procedure can be omitted if they are not relevant, and carried out thoroughly or partially as appropriate.

### 6.3 Data protection requirements

All data protection requirements whose observance the inspector may have to check can be analysed under these headings:

- notifications:
  - particulars of the system must be disclosed to:
    - the Data Protection Authority
    - the data subjects
    - the public
  - the contents of a data subject's record must be disclosed to him in a form which the layman can understand
  - a licensing or registration fee may be required
- data quality: the data must be:
  - true
  - accurate
  - sufficient
  - necessary
  - not misleading
  - up-to-date



- the data processes must be legitimate:
  - the purposes of the system must be acceptable
  - the individual processes in the system must be fair to all interested parties
- the processes must be carried out without error
- there must be no access to personal data other than for approved purposes
- the personnel who operate the system must be informed of their data protection responsibilities, and given the means and encouragement to carry them out
- there should be controls in the data system to provide checks on its working, so that malfunctions of any sort can be detected, and, if appropriate, overcome.

These requirements can be expanded into a set of measures that the system should perform, with corresponding checkpoints which the inspector can investigate.

#### 6.4 The inspection procedure

Usually the inspector will contact the person responsible for the system beforehand, to agree an outline plan for the inspection, and to ask for preliminary information.

Unannounced inspections should occur only if there is reason to suspect a serious breach of the data protection regulations, which must be stopped quickly, or for which the evidence may disappear if the inspection is delayed. The inspector will use the preliminary information to plan his on-site inspection. In principle he may inspect all parts of the system to check compliance with all aspects of the requirements referred to in the previous section, but usually he will select parts and aspects which in his opinion are important.

When the inspector has analysed the information which he has collected, he writes a report stating his findings on the degree of compliance of the system with the data protection regulations. He may make recommendations and give advice (either informally during his inspection visit, or in his report) on how the system could and should be improved from the point of view of data protection, but only in a way which does not compromise his independence.

The inspection report should be shown to the person responsible for the system unless this might prejudice legal proceedings against him; in any case he should be told the main findings. There is a case of publishing the report, with exclusions to protect the data user's necessary secrets.

## 6.5 The inspector

The inspector requires the following qualities:

- understanding of data protection
- experience in the way human beings in organisations work
- knowledge of the technology used in the system
- general inspection skills
- trustworthiness.

No existing profession demands all these, and people possessing them are rare.

A statutory inspection team should normally consist of more than one person, to provide a spread of the necessary qualities, to allow them to check each other, and to increase the objectivity of the inspection.

Particularly in a statutory inspection, the inspector needs special powers to obtain information, and he must be clearly given these powers and supported in exercising them. In some cases he may be exposed to various pressures to distort his judgement, and must be supported against them. But there must be a means of complaint against an inspector who has exceeded or misused his powers, or made a mistake.

## 6.6 Conclusion

This examination of the inspection process has shown that all the legal requirements for data protection can be inspected, has suggested a practical set of steps for checking compliance, and has produced no reason for believing that serious breaches of the law would be easy to operate without detection.

The public concern over the uses of personal data, which has led to data protection laws, justifies the existence of a substantial, effective and visible inspection activity.

## 7 Conclusion

### 7.1 General observations

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

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

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

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

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

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

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

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

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

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

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

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

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



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

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

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

## 7.2 Co-operation between the institutes

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

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

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

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

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

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

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

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

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

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

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

### 7.3 Further studies

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

1. Nations with data protection legislation can review it in the light of the experience of their data inspection agencies and public opinion. This seems to lead to the exemption of trivial data processing, and to easier procedures for the commonest data banks which contain data that does not seem dangerous. At the same time, a more careful approach is being made to specify sectors of data processing like public health, social security, employment agencies, research and national security. Among these sectors, all except perhaps the last deserve the attention of the EEC, since it is not altogether clear what consequences this more sectoral approach will have.
2. Though international regulations have been drafted, it is not clear when and how the different nations will respond to them, and how practical they will prove in day-to-day data traffic. This is of especial importance with regard to data traffic between EEC and non-EEC countries. This uncertainty is partly due to

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

3. The scope of data protection has grown widely in recent discussions. Issues like the balance of power, employment, national sovereignty, freedom of information, the 'New World Information Order' and economic dependency have been closely mingled with the former issues of privacy and openness. This enlargement of issues has led to controversies on data protection issues, and has widened the considerations for regulations to non-physical legal entities, as well as to economic data. The consequences of these complications for existing data protection regulation, and for the whole issue of information as an economic good have not yet been sufficiently analysed.
4. While regulation activities have reached some degree of consolidation, technological development has not stopped. It is still dubious how existing national and international regulations can react to new developments like satellite communication and micro-computers.

5. In addition to existing regulations, there are still more far-reaching proposals for regulating information flows and giving undue protectionism that must not be ignored in further policy-making. This applies mainly to the recommendations of the European Parliament, but also to further activities of the Council of Europe in the area of access to government data. Whereas the former poses legal and organisational problems whose extent remains to be analysed, the latter may become important to present data protection regulations, and may pose problems of competition, as experiences with the U.S. Freedom of Information Act suggest.
6. Furthermore, the economic consequences of the drafted and proposed international agreements are far from being clear and demand further study.
7. Another issue which has been observed, but not explored, during the present study, is the influence of tariffs and regulatory aspects of telecommunications in the development of information flows.

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

1. Technical problems of ensuring privacy, and data protection problems arising from new technologies
2. Data protection rights of the EEC citizen
3. Data protection and organisational policy
4. Possible role and structure of a European data protection control body
5. Economic aspects of harmonization procedures
6. Protection of research data
7. Transferability of data protection models
8. Assessment of information policy and legal problems with regard to telecommunications and data flows between EEC and non-EEC countries.



#### 7.4 Acknowledgement

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

## Contents of section 1

- 1.0 Introduction
  - 1.0.0 Foreword
  - 1.0.1 Aim
  - 1.0.2 Methodology of the survey
  - 1.0.3 Analysis of the results
  
- 1.1 TBDF: general presentation
  - 1.1.0 Introduction
    - 1.1.1 Computer networks
      - 1.1.1.1 Batch processing
      - 1.1.1.2 Timesharing networks
    - 1.1.2 Specialised networks
      - 1.1.2.1 SITA: the airlines network
      - 1.1.2.2 SWIFT
      - 1.1.2.3 EUREX
    - 1.1.3 International business and the management of large groups
      - 1.1.3.1 Management of accounts and finance
      - 1.1.3.2 Management of production and stocks
      - 1.1.3.3 Purchase, sales and delivery orders
      - 1.1.3.4 Statistics and commercial forecasts
      - 1.1.3.5 Research and development
      - 1.1.3.6 Exploitation of a centralised file
    - 1.1.4 Hotel and travel bookings, car hire
    - 1.1.5 The press
      - 1.1.5.1 Associated Press
      - 1.1.5.2 Reuters
    - 1.1.6 The Preparation of data and transfer of programs
      - 1.1.6.1 Data preparation
      - 1.1.6.2 Program transfers
    - 1.1.7 Scientific and technical cooperation
      - 1.1.7.1 Meteorological forecasts: the World Meteorological Organisation
      - 1.1.7.2 An example of collaboration in computing: EIN
      - 1.1.7.3 Some examples of data banks
    - 1.1.8 Data banks and data bases
      - 1.1.8.1 The American systems: DIALOG and ORBIT
      - 1.1.8.2 The European Space Agency
      - 1.1.8.3 The EURONET network
      - 1.1.8.4 DATA RESOURCES Inc.
      - 1.1.8.5 CHASE ECONOMETRICS
    - 1.1.9 Administrative and governmental data flows
  
- 1.2 Classification of TBDF
  - 1.2.0 Introduction
  - 1.2.1 Criteria of classification
  - 1.2.2 Transfer medium
  - 1.2.3 The character of the operator
  - 1.2.4 The nature of the information carried
  - 1.2.5 Direction of the exchanges
  - 1.2.6 Commercial and non-commercial flows
  - 1.2.7 Material flows: postal and customs position
  - 1.2.8 Non-material flows: the telecommunications regulatory administration

- 1.3 The amount of TBDF
  - 1.3.1 Interest in the amount of data flows
  - 1.3.2 Difficulties encountered during the survey
  - 1.3.3 Some quantitative aspects of TBDF
  - 1.3.4 The basic problem: evaluation of data flows
    - 1.3.4.1 Measure of volume
    - 1.3.4.2 Measure of value
- 1.4 Conclusion
- 1.5 Bibliography
  - 1.5.1 Legal aspects of transborder data flows
  - 1.5.2 OECD documents
  - 1.5.3 Networks and transborder data flows
  - 1.5.4 Data banks, information retrieval networks
  - 1.5.5 Telecommunications satellites
  - 1.5.6 UNESCO documents
  - 1.5.7 Other interesting sources

## Contents of section 2

### 2.0 Introduction

#### 2.0.1 Definition of the item

#### 2.0.2 Scheme of the report and methodological problems

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

#### 2.1.0 Preliminary remarks

#### 2.1.1 Belgium

##### 2.1.1.1 Present legislative position

##### 2.1.1.2 Data protection law as a context to the control authority

##### 2.1.1.3 Control authority

#### 2.1.2 Denmark

##### 2.1.2.1 Present legislative position

##### 2.1.2.2 Data protection law as a context to the control authority

##### 2.1.2.3 Control authority

#### 2.1.3 France

##### 2.1.3.1 Present legislative position

##### 2.1.3.2 Data protection law as a context to the control authority

##### 2.1.3.3 Control authority

#### 2.1.4 United Kingdom

##### 2.1.4.1 Legislative position

##### 2.1.4.2 Data protection law as a context to the control authority

##### 2.1.4.3 Control authority

#### 2.1.5 Ireland and Italy

#### 2.1.6 Luxemburg

##### 2.1.6.1 Present legislative position

##### 2.1.6.2 Data protection law as a context to the control authority

##### 2.1.6.3 Control authority

#### 2.1.7 The Netherlands

##### 2.1.7.1 Present legislative position

##### 2.1.7.2 Data protection law as a context to the control authority

##### 2.1.7.3 Control authority

### 2.2 Data protection authorities in the German Federal Republic and Sweden

#### 2.2.0 Introduction

#### 2.2.1 The data protection system of the German Federal Republic

##### 2.2.1.1 The federal structure of the system

##### 2.2.1.2 Control authorities and the Federal Data Protection Law

###### 2.2.1.2.1 Present legislative position

###### 2.2.1.2.2 Data protection law 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 transborder data flow
      - 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
    - 2.5.0 Preliminary remarks
    - 2.5.1 Crucial points within the scope of the present study
    - 2.5.2 Related problems
  - 2.6 Bibliography

Illustrations

  - Organisational structure of Swedish DIB
  - Level of decision-making
  - Development of the budget
  - Activities of the DIB

## Contents of section 3

- 3.1 Introduction
- 3.2 Extension of protection to non-physical persons: view of the people concerned
  - 3.2.1 The legal status of the business
  - 3.2.2 The size of the business
    - 3.2.2.1 Reactions of large companies in their business relations
    - 3.2.2.2 Reactions of large and small companies in their business relations
  - 3.2.3 The public or private nature of non-physical person files
- 3.3 Distinction between the two problems
  - 3.3.1 First problem: how far does protection of physical persons extend?
  - 3.3.2 Second problem: should non-physical persons actually be protected?
- 3.4 Specificity of the files of non-physical persons
  - 3.4.1 Significance of the concept of non-physical person
  - 3.4.2 Nature of the data on non-physical persons
    - 3.4.2.1 Public data
    - 3.4.2.2 Revealed data
    - 3.4.2.3 Gleaned information
    - 3.4.2.4 Derived information
    - 3.4.2.5 Information obtained by spying
  - 3.4.3 Protection necessary for non-physical persons
    - 3.4.3.1 The requirement of secrecy
    - 3.4.3.2 Publicity regulations on non-physical persons
    - 3.4.3.3 Difficulties connected with computer files
- 3.5 Effective protection for physical persons
  - 3.5.1 The case of mixed files
  - 3.5.2 Files containing indirect information about physical persons
- 3.6 Conclusions and European outlook
- 3.7 Bibliography

## Contents of section 4

- 4.        INTERNATIONAL ECONOMIC ASPECTS OF DATA PROTECTION
  
- 4.1       DEFINITION OF THE PROBLEM AND SUMMARY
- 4.1.1     Definition of the problem
- 4.1.2     Summary
  
- 4.2       Concepts of economic theory and methodology
- 4.2.1     Problems of the application of concepts of economic theory to the analysis of costs and profit margins
- 4.2.1.1   Data protection as a "public benefit" : The problem of the determination of the benefit
- 4.2.1.2   External and Alternative Costs: Difficulties of Determination
- 4.2.1.3   The fundamental positional value of relevant national economic concepts
- 4.2.2     Limitation to costs and profits on the basis of business economics
- 4.2.3     Methodological method of procedure
  
- 4.3       Costs of data protection : Estimates and experience in selected countries
- 4.3.1     Great Britain
- 4.3.1.1   General Data Protection Debate

- 4.3.1.2 Special Cost Estimates
- 4.3.1.3 The Report of the Committee on Data Protection
  - 4.3.1.3.1 User Costs: The Study of PACTEL
    - 4.3.1.3.1.1 Terms of Reference
    - 4.3.1.3.1.2 Conception and methodological Procedure
    - 4.3.1.3.1.3 Results and Evaluation of the Study
    - 4.3.1.3.1.4 Conclusions of the Committee on Data Protection
  - 4.3.1.3.2 Information Fees
  - 4.3.1.3.3 Registration Fees of the Data Protection Authority
- 4.3.1.4 Summary
  
- 4.3.2 U S A
  - 4.3.2.1 Data Security Discussion
  - 4.3.2.2 Analysis of the Goldstein Privacy Estimation Model
    - 4.3.2.2.1 Structure and Function of the Model
    - 4.3.2.2.2 Application of the Model
    - 4.3.2.2.3 Evaluation and Results of the Study
      - 4.3.2.2.3.1 Data Protection Cost Structure
      - 4.3.2.2.3.2 Industry Aspects
      - 4.3.2.2.3.3 User Aspects
    - 4.3.2.2.4 Conclusions



- 4.3.2.3 Experience with the Privacy Act
  - 4.3.2.3.1 Cost Survey of the Office of Management and Budget
  - 4.3.2.3.2 Analysis of the Results
  - 4.3.2.3.3 Consequences
  
- 4.3.3 Sweden
  - 4.3.3.1 Licensing Charge
  - 4.3.3.2 Information requests
    - 4.3.3.2.1 Extent of the information requests
    - 4.3.3.2.2 Costs of giving information
    - 4.3.3.2.3 Information fees
  - 4.3.3.3 Data security measures
  - 4.3.3.4 Loss of opportunity for earnings
  - 4.3.3.5 Positive consequences of the Data Law
  - 4.3.3.6 International Competition Distortion
  - 4.3.3.7 International Data Harmonisation
  - 4.3.3.8 General Viewpoint of the Swedish Industrial Federation
  
- 4.3.4 German Federal Republic
  - 4.3.4.1 Estimation of costs before the coming into force of the Federal Data Protection Law
  - 4.3.4.2 Cost-related Experience with the Federal Data Protection Law

- 4.3.4.2.1 Data Protection Authorized and Data Protection Training
- 4.3.4.2.2 Obligation to advise
- 4.3.4.2.3 Information requests
  - 4.3.4.2.3.1 Volume and costs of information requests
  - 4.3.4.2.3.2 Information charges
- 4.3.4.2.4 Data Security Measures
- 4.3.4.2.5 Summarisation and Considered Thoughts
  
- 4.4 Costs of Data Protection: General Conclusion
  - 4.4.1 Over-estimation of Data Protection Costs
  - 4.4.2 Advising
  - 4.4.3 Information requests
  - 4.4.4 Data Protection Authorized Officers and other Data Protection Personnel Costs
  - 4.4.5 Registration and Licensing Fees
  - 4.4.6 Data Security
  - 4.4.7 Opportunity Costs
  - 4.4.8 Effects with regard to cost and other positive effects for the data processing agencies
  
- 4.5. The Problems of International Competition
  - Distortions caused by Data Protection Costs
    - 4.5.1 The problem stated

- 4.5.2 Evaluation of the competition problem
- 4.5.3 Judgement from the point of view of the data subject
  
- 4.6 Cost-effective Harmonisation Measures of a European Data Protection Policy
- 4.6.1 Cost-relevant elements of a data protection harmonisation policy
  - 4.6.1.1 Principles
  - 4.6.1.2 Registration and licensing
  - 4.6.1.3 National data protection authorities
  - 4.6.1.4 Notification
  - 4.6.1.5 Granting of information
  - 4.6.1.6 Data security
  - 4.6.1.7 Data protection supervisor and data protection liability
- 4.6.2 Costs of data protection harmonisation
  
- 4.7 Possible Main Points of Emphasis of Future Research Orientated towards the Economy
- 4.7.1 Accompanying research for the preparation and implementation of European data protection guidelines
- 4.7.2 Economic aspects of the data protection of corporate bodies
- 4.7.3 Legal framework of a European common data and information market

## Contents of Section 5

### 5.0 Introduction

#### 5.1 Technical context and long-term trends

##### 5.1.1 Hardware development

##### 5.1.2 Software

##### 5.1.3 The appearance of the electronic office

##### 5.1.4 Attempts at standardisation

#### 5.2 Should the public know of the existence of files?

#### 5.3 Should the individual know of the existence of information concerning him in a file?

##### 5.3.1 Notification methods

##### 5.3.2 Access methods

#### 5.4 Should the individual know the information about him in a file?

##### 5.4.1 Initiation of the request

##### 5.4.2 Reply to the request or notification

###### 5.4.2.1 The essential components of a system

###### 5.4.2.2 Defining information about an individual

###### 5.4.2.3 Retrieval of information connected with an individual

###### 5.4.2.4 Presentation of the results

#### 5.5 Can the information be corrected?

### 5.6 Conclusion

### 5.7 Bibliography

## Contents of section 6

- 6.0 Introduction
  - 6.0.1 The motivation for this item
  - 6.0.2 The purposes of inspection
  - 6.0.3 Structure of section 6
  - 6.0.4 Referencing system
  
- 6.1 Definitions
  - 6.1.0 Introduction
  - 6.1.1 Definition of 'organisation'
  - 6.1.2 Definition of 'system'
  - 6.1.3 Definition of 'data user'
  - 6.1.4 Definition of 'data', 'data subject', 'information'
  - 6.1.5 Definition of 'regulations'
  - 6.1.6 Definition of 'commissioning body', 'Authority'
  - 6.1.7 Definition of 'inspection', 'inspection visit', 'inspection report'
  - 6.1.8 Definition of 'inspector'
  
- 6.2 Preliminary questions
  - 6.2.0 Introduction
  - 6.2.1 Actual and potential breaches
  - 6.2.2 Selection of inspection areas
  - 6.2.3 The powers of the inspector
  - 6.2.4 Statutory and voluntary inspections
  - 6.2.5 An inspection paradox
  - 6.2.6 Strictness
  - 6.2.7 Global uniformity
  
- 6.3 The principles of data protection
  - 6.3.0 Introduction
  - 6.3.1 Notifications
    - 6.3.1.0 Introduction
    - 6.3.1.1 Particulars of the system
    - 6.3.1.2 Data subject's access to his record
    - 6.3.1.3 Registration fee
  - 6.3.2 Data quality
  - 6.3.3 Legitimate processes
  - 6.3.4 Restricted access
  - 6.3.5 Personnel
  - 6.3.6 Control
  
- 6.4 The inspection: preparation
  - 6.4.0 Introduction
  - 6.4.1 Initiation of the inspection
  - 6.4.2 Factors conducive to inspection
  - 6.4.3 What is the system?
  - 6.4.4 Charging the inspector
  - 6.4.5 Timing of an inspection
  - 6.4.6 Approach to the organisation
  
- 6.5 The inspection: information gathering
  - 6.5.0 Introduction
  - 6.5.1 Preliminary information
  - 6.5.2 Personnel
  - 6.5.3 Notifications
  - 6.5.4 Data capture
  - 6.5.5 Data preparation

- 6.5.6 Data quality
- 6.5.7 Restricted access
- 6.5.8 Data update
- 6.5.9 Data use
- 6.5.10 Data interrelation
- 6.5.11 Data dissemination
- 6.5.12 Data archival
- 6.5.13 Data erasure
- 6.5.14 Control
  
- 6.6 The inspection: conclusion
  - 6.6.0 Introduction
  - 6.6.1 Presentation of the inspection report
  - 6.6.2 Contents of the inspection report
  - 6.6.3 Subsequent actions by the commissioning body
  - 6.6.4 The inspector's other findings
  - 6.6.5 Disposal of inspection materials
  
- 6.7 The inspector
  - 6.7.1 The inspector's qualities
  - 6.7.2 Who should inspect?
  - 6.7.3 Relation to financial auditing
  - 6.7.4 Questions of judgement
  - 6.7.5 Pressures on the inspector
  - 6.7.6 How helpful should the inspector be?
  - 6.7.7 Complaints against the inspector
  - 6.7.8 The inspector's answerability
  
- 6.8 Further considerations
  - 6.8.0 Introduction
  - 6.8.1 Frequency of inspection
  - 6.8.2 Strictness of inspection
  - 6.8.3 Attitude of data user
  - 6.8.4 Secrecy of inspection procedure
  - 6.8.5 Publication of the inspection report
  - 6.8.6 Inspecting the Authority
  - 6.8.7 The cost of the inspection
  - 6.8.8 Determination of the regulations
  - 6.8.9 Relation to security
  - 6.8.10 International aspects
  - 6.8.11 Computer bureaux
  - 6.8.12 Non-standard operations
  - 6.8.13 Sources of information
  - 6.8.14 Inspecting databases
  - 6.8.15 Undisclosed systems
  - 6.8.16 Length of inspection visit
  
- 6.9 Acknowledgements and references
  - 6.9.1 Acknowledgements
  - 6.9.2 References

## Illustrations

- Statutory and voluntary inspections
- Notice of inspection
- Model of inspection report
- Letter following inspection