CONSEQUENCES OF

DATA PROTECTION LEGISLATION

H. van Tongeren, IBM Europe
Tour Pascal, Cedex 40,
F-92075 Paris - La Defense
France. Tel: 33-1-767 61 79

C O N S E Q U E N C E S O F
D A T A P R O T E C T I O N L E G I S L A T I O N

1. WHAT IS DATA PROTECTION LEGISLATION REALLY ABOUT ?

It seems sensible to start a discussion of the consequences of data protection legislation with the question what this legislation is really about. Looking at the existing national law in Europe, one comes sooner or later to the conclusion that the answer to that question is not self-evident.

1.1 The titles of the national data protection acts

It may be of interest to look at the titles of the different acts: do they tell us something about their purpose and contents?

- Some of them are called just "data" or "files" act, sometimes with the addition of "personal" (e.g. Denmark, Norway, Sweden).

- Others are more precise, or: more limitative?, in using "data protection", with or without "personal" (e.g. Austria, Germany, U K).

- Those using the French language are more imaginative. The Luxemburg act shifts from "data protection" to "data use": "Loi réglementant l'utilisation des données nominatives dans les traitements informatiques". In the title of the French act, we see for the first time the suggestion of a wider view: "Loi relative à l'informatique, aux fichiers et aux libertés".

- The "subtitle" of the UK act comes very close to the title of the Luxemburg act: "An Act to regulate the use of automatically processed information relating to individuals and the provision of services in respect of such information."

Conclusion: in their titles, these acts state primarily that they address the issue of personal information, handled through some kind of automated information processing (definition of "data").

1.2 The titles of international instruments

The two international data protection instruments are much more explicit:

- OECD: "Guidelines on the protection of privacy and transborder flows of personal data".

- Council of Europe: "Convention for the protection of individuals with regard to automatic processing of personal data".

In these titles, there is an interesting shift from "protection of (personal) data" to "protection of privacy / individuals".

1.3 Statements of principle in national acts

In contrast to the matter-of-fact titles, some of the national acts contain explicit statements about the main principles that are, or are intended to be, addressed by the legislation. Let me quote some phrases:

- Austria: "Jedermann hat Anspruch auf Geheimhaltung der ihn betreffenden personbezogenen Daten, soweit er daran ein schutzwürdiges Interesse, insbesondere im Hinblick auf Achtung seines Privat- und Familienlebens, hat."

- Germany: "Aufgabe des Datenschutzes ist es, durch den Schutz personenbezogener Daten vor Missbrauch bei ihrer Speicherung, Uebermittlung, Veränderung und Löschung (Datenverarbeitung) der Beeinträchtigung schutzwürdiger Belange der Betroffenen entgegenzuwirken."

- France: "L'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques."

In such statements, one finds the expression of broad human rights and the need to protect individual and family life against the possible misuse of personal information.

1.4 A mixture of principles and approaches

Of course, titles and statements of principle reveal only some aspects. In order to really decide what these acts are about, one has to analyze their full contents, which is outside the scope of this paper. However, having worked for a number of years with these acts in practical life I have become convinced of a fact, which is already suggested by their titles and statements of principle: it is not possible to define simply and clearly what these acts are about. They all show a somewhat confusing mixture of principles and approaches. In every act, one can identify always some, and sometimes all, of the following purposes:

- Definition of a Human Right: the right to protection of individual (and family) life.

- Legal protection of individuals' privacy.

- Legal protection of individuals' and legal persons' privacy.

- Legal protection of individuals against the misuse of information about them.

- Legal protection of individuals and legal persons against the misuse of information about them.

- A legislated "code of conduct" for the handling of (personal) information.

- Protection of national commercial interests.

It is this mixture of intentions that makes it so difficult to assess what the consequences of data protection legislation are or should be.

1.5 The contents of the national data protection acts

The mixture of intentions and approaches is reflected by the acts' contents, which always cover a variety of aspects. Fig. 1 contains a, simplified, comparative overview of main aspects of the laws enacted 1973 through 1981.

In general, one can recognize the following main sections:

- Constitutional / basic right(s), purpose
- Definitions, scope
- Data subject rights
- Data (file) controller (user) obligations
- Administrative control system
- Sanctions (penal / civil law).

Besides these general sections, an act may address one or more specific areas, such as:

- Eaves-dropping, etc.
- Transborder access / processing
- Service bureaus
- Credit referencing
- Direct mail.

2. HOW DATA PROTECTION LEGISLATION CAN BE PERCEIVED

As discussed in the previous chapter, the European data protection acts consist of a mixture of rights and principles, of more or less detailed rules and regulations, and of an administrative control system. It is, therefore, not evident what this legislation wants to achieve. As a result, the consequences of data protection legislation depend to a great extent on how this law is perceived by society.

Very schematically, one can say that this legislation and, therefore, its consequences for the Data Controllers (Users) can be perceived in three different ways:

a) A new form of bureaucracy.

Consequence: the minimum compliance that is necessary to ensure adherence to the legal requirements:

- Understand the administrative requirements issued by the Data Inspectorate (Registrar).
- Fill out the necessary forms, submit them to the Data Inspectorate and file copies.

b) A new form of business / administration practices.

Consequence: in addition to a), the minimum compliance that is necessary to ensure adherence to company requirements:

- Establish internal procedures and administration.

c) A new form of "informatics" ethics:

Consequence: in addition to a) and b), define internal principles and practices:

- Establish an internal "code of conduct"
- Inform, educate, convince.

3. WHAT SHOULD THE CONSEQUENCES BE ?

3.1 The recommended approach

We recommend the approach as defined under 2.c) above, for two main reasons:

- In today's and tomorrow's world, information technology will play an increasingly important role and will, therefore, have a direct effect on society and individual citizens. Data Controllers (Users) have a moral obligation to consider how their collection, use and dissemination of information in general, and of personal information in particular, influences society and data subjects.

- It is to be expected that both individual data subjects and data subject organizations such as civil rights associations, consumer organizations, unions, work councils, etc. will use the data subject's legal rights to ensure a careful and responsible handling of personal information.

3.2 The practical consequences

What are, then, the practical consequences for any Data Controller, whether company, association, government agency, university, etc.? We recommend the following:

a) Establish the minimal organization / administration that is needed in order to:
   - ensure adherence to internal principles / practices
   - ensure compliance with legal requirements
   - fulfill the bureaucratic requirements.

b) Define the internal principles and practices.
   (Take as minimum the principles outlined by:
   - the national legislation
   - the different national acts
   - the international instruments.)

c) Inform management and employees:
   - Publish easy-to-read information material
   - Inform, educate, instruct.

   (Fig. 2 - 3 show two pages from an IBM publication. Fig. 2 tries to explain the company's main principles and practices, while Fig. 3 summarizes its position on the scope of data protection).

d) Ensure adherence to internal principles and practices:

- Define responsibilities

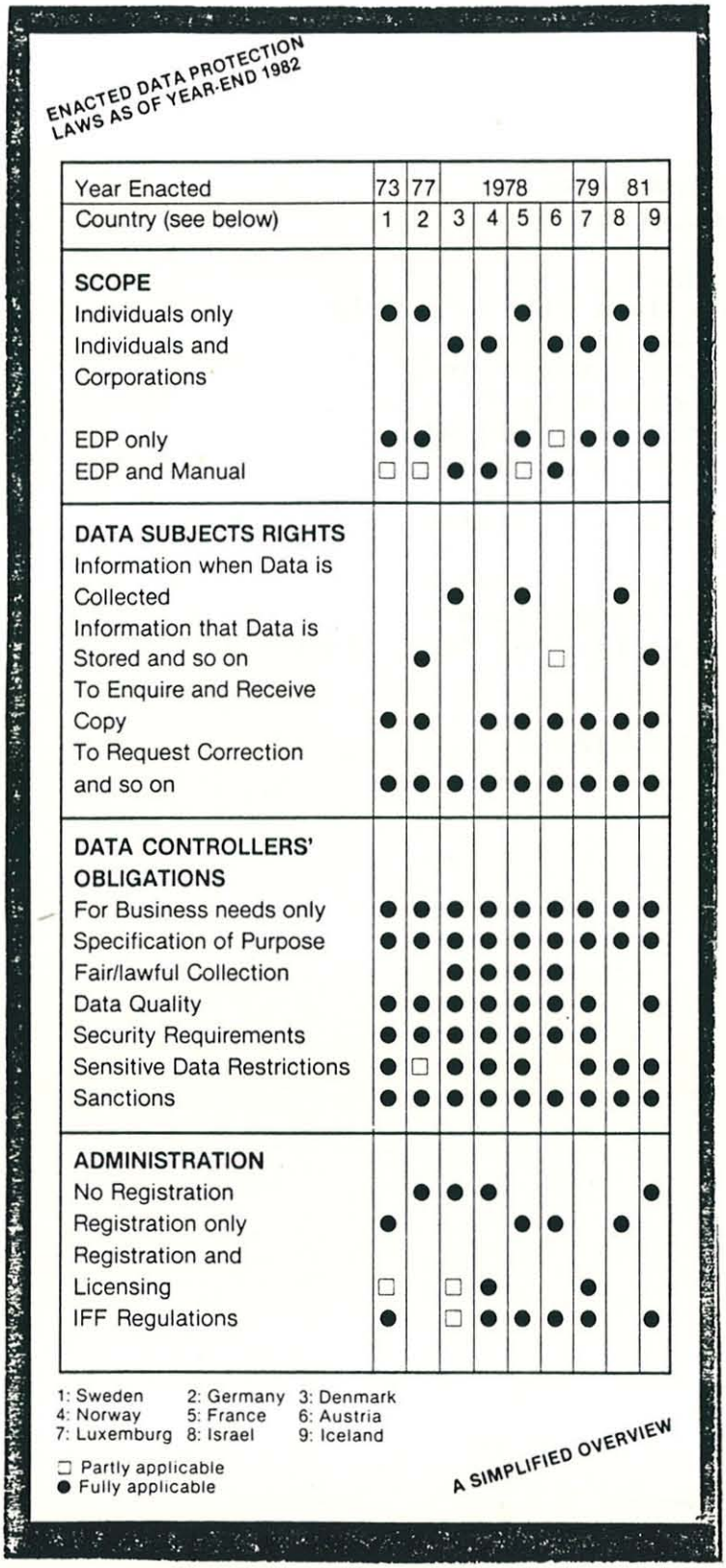
- Publish easy-to-use checklists; e.g.:

  - well defined purpose(s) and owner
  - well defined data sources, providers and collection methods
  - necessary data elements only
  - necessary (categories of) data subjects only
  - well defined processing (applications)
  - need-to-know data receivers / users only
  - adequate information systems security
  - well defined procedures for handling of data subject requests.

e) Understand the legal / administrative requirements. E.g.:

- forms to be filled out (Data Inspectorate)
- approval to be obtained (Data Inspectorate)
- requests for information to be handled (Data Inspectorate and Data Subjects)

and establish the necessary procedures.



ENACTED DATA PROTECTION LAWS AS OF YEAR-END 1982

Year Enacted	73	77	1978				79	81	
Country (see below)	1	2	3	4	5	6	7	8	9
SCOPE									
Individuals only	●	●			●			●	
Individuals and Corporations			●	●		●	●		●
EDP only	●	●			●	□	●	●	●
EDP and Manual	□	□	●	●	□	●			
DATA SUBJECTS RIGHTS									
Information when Data is Collected			●		●			●	
Information that Data is Stored and so on		●				□			●
To Enquire and Receive Copy	●	●		●	●	●	●	●	●
To Request Correction and so on	●	●	●	●	●	●	●	●	●
DATA CONTROLLERS' OBLIGATIONS									
For Business needs only	●	●	●	●	●	●	●	●	●
Specification of Purpose	●	●	●	●	●	●	●	●	●
Fair/lawful Collection			●	●	●	●			
Data Quality	●	●	●	●	●	●	●		●
Security Requirements	●	●	●	●	●	●	●		
Sensitive Data Restrictions	●	□	●	●	●		●	●	●
Sanctions	●	●	●	●	●	●	●	●	●
ADMINISTRATION									
No Registration		●	●	●					●
Registration only	●				●	●		●	
Registration and Licensing	□		□	●			●		
IFF Regulations	●		□	●	●	●	●		●

1: Sweden 2: Germany 3: Denmark
4: Norway 5: France 6: Austria
7: Luxemburg 8: Israel 9: Iceland

□ Partly applicable
● Fully applicable

A SIMPLIFIED OVERVIEW

FIG. 1

PROTECTION OF PERSONAL DATA
MAIN PRINCIPLES AND PRACTICES

- THE PURPOSE FOR WHICH PERSONAL DATA IS USED MUST BE CLEARLY DEFINED AND SHOWN TO BE IN SUPPORT OF VALID BUSINESS NEEDS.
- ONLY PERSONAL DATA THAT ARE RELEVANT TO THE DEFINED PURPOSE(S) MAY BE COLLECTED, STORED, RETAINED, PROCESSED, AND COMMUNICATED.
- PERSONAL DATA MUST BE COLLECTED BY FAIR AND LAWFUL MEANS FROM RELIABLE SOURCES.
- PERSONAL DATA MUST BE CORRECT, COMPLETE, AND UP-TO-DATE.
- WITHIN THE DATA CONTROLLER'S ORGANIZATION PERSONAL DATA MAY BE AVAILABLE ONLY TO DATA USERS WITH A WELL-DEFINED NEED-TO-KNOW.
- TO THIRD PARTIES, PERSONAL DATA IS TO BE COMMUNICATED ONLY:
  - WHEN REQUIRED FOR VALID BUSINESS REASONS, AND
  - WHEN LEGALLY PERMITTED, AND
  - IF LIMITED TO THE DATA REQUIRED, AND
  - IF THE RECEIVER GUARANTEES EQUIVALENT PROTECTION.
- WHENEVER FEASIBLE, PERSONAL DATA IS TO BE PROCESSED AND COMMUNICATED IN AGGREGATE OR ANONYMOUS FORM IN ORDER TO AVOID IDENTIFICATION OF THE DATA SUBJECTS.
- ALL INFORMATION CONTAINING PERSONAL DATA MUST BE CAREFULLY CLASSIFIED, AND PROTECTED AGAINST UNAUTHORIZED OR ACCIDENTAL DISCLOSURE, MODIFICATION, OR DESTRUCTION.
- DATA SUBJECTS SHOULD BE ALLOWED TO REVIEW THE RELEVANCE AND THE ACCURACY OF DATA RELATED TO THEM.

FIG. 2

PROTECTION OF PERSONAL DATA
SCOPE

- ALL PERSONAL DATA SHOULD BE PROTECTED, REGARDLESS OF DATA HANDLING METHODS AND TECHNIQUES.
- WELL MANAGED, COMPUTERIZED INFORMATION SYSTEMS, WITH EFFECTIVE DATA SECURITY, MAY WELL OFFER THE BEST PROTECTION OF PERSONAL DATA.
- PERSONAL DATA IS OFTEN LESS WELL PROTECTED IN MANUAL FILES.

➧ PERSONAL DATA PROTECTION PRINCIPLES AND PRACTICES SHOULD APPLY TO BOTH COMPUTERIZED AND MANUAL DATA.

- PERSONAL DATA PROTECTION IS PRIMARILY CONCERNED WITH THE PROTECTION OF THE RIGHTS OF INDIVIDUALS.

➧ NATIONAL DATA PROTECTION LEGISLATION SHOULD PROTECT INDIVIDUALS AGAINST THE MISUSE OF THEIR PERSONAL DATA.

HOWEVER:

- EACH EMPLOYEE, CUSTOMER, SUPPLIER, AND SO ON HAS THE RIGHT TO EXPECT THAT A DATA CONTROLLER CAREFULLY MANAGES ALL DATA RELATED TO HIM.
- IT CAN BE DIFFICULT TO DRAW A LINE BETWEEN INDIVIDUALS AND COMPANIES. FOR EXAMPLE: ONE-MAN COMPANIES, PARTNERSHIPS, OR ASSOCIATIONS.
- FILES AND APPLICATIONS OFTEN USE DATA RELATED TO MANY DIFFERENT KINDS OF DATA SUBJECTS.

➧ WITHIN A DATA CONTROLLER'S ORGANIZATION, PERSONAL DATA PROTECTION, PRACTICES, AND PRINCIPLES SHOULD APPLY TO ALL DATA SUBJECTS.

FIG. 3

DISCUSSION

Professor Griffiths said that French Data Protection law administration seems to be way behind the actual terms of the act, and asked whether this was standard throughout Europe.

The speaker replied that this is due to the fact that besides an act itself, one needs to set up practical administrative machinery to make it work. For instance, if the act itself is vague, it has to be decided whether to include manual records as well as computer records. In Luxembourg, thousands of forms were sent out for people to fill in, then nothing happened for a long time. In practice, it appears that about three years are required to get things under control.

Mr. Dunlop asked how IBM dealt with awkward cases such as data on citizen A accessed in country B using a computer in country C.

Mr. van Tongeren replied that IBM France tends to use French law etc., but the problem of trans-border data flow is tricky. In practice, one has to work in such a way as to uphold the law of each country involved. This has to be carefully devised beforehand to be as general as possible.

Mr. Amery pointed out that a citizen of Australia can be affected by U.K. data about him, and data doesn't have to move.

Professor Randell asked about inconsistencies between different countries' laws. The speaker replied that if you read the various laws, they do appear to be quite different. However, in practice, they are not really very different when administered.