

Keywords to Proposals,

Among the proposals in this report the following may be especially emphasized:

- * Greater freedom to register and handle general personal information - accompanied with the right for the registered person to obtain insight into his case.
- * A new judicial principle in the field of general personal information. The present principle makes all personal data-registration illegal unless permitted. It is suggested that this principle be changed to the opposite: registration is permitted unless it is prohibited.
- * The making of data-laws which liberalize registration, usage and passing-on of general personal information but which at the same time tighten up the rules for treating confidential and strictly private information.
- * A new technique for legislation via a general law on the protection of personal data, and rules for personal protection of sensitive data in special areas of legislation which regulate different fields of the society.
- * Rejection of superior and general EU-rules for exchange of data across the borders?
- * Initiation of research which should disclose the present opinion of the general population on the use of registers - including scope, depth and direction of the conception: "fear-of-registers".
- * Strengthening of the Danish Data Surveillance Authority (Registertilsynet). The Data Surveillance Authority should be more independent of the government and the Department of Justice and should take part in the debate.

NB.: In the present report three categories of personal information are to be kept separate: general, confidential and strictly private personal information.

The Register Work Group

The report has been worked out by a group of experts established under the Danish Board of Technology. The Register Work Group was composed by the following:

- Mads Bryde Andersen, Professor, Doctor of laws; The University of Copenhagen.
- Oluf Jørgensen, LLB, Reader,- The University of Aalborg
- Alex Frank Larsen, Journalist, Editor of 'Kontakt'.
- Jørn Ravn, Head of the Secretariat at the Danish Board of Technology.
- Steffen Stripp, Information Technology Consultant
- Jan Aagaard, BCom, Head of department,- The Municipality of Esbjerg

The members of the Register Work Group do not act as representatives of the institutions at which they are employed. The Work Group has not been composed in order to obtain consensus, but rather to ensure a broad treatment of those elements in the Danish data legislation which need to be taken up for discussion.

Tasks and Methods

In the autumn of 1992, The Danish Board of Technology decided to collect material for an evaluation of the set of values which is included, or ought to be included in the Danish legislation regarding edp-related personal registers.

- Which considerations should be taken?
- How should the consideration towards personal integrity of the individual be weighted against society's need for security, control and effectiveness in the government services?
- How should modern legislation relate itself to an explosive technological development which opens up new possibilities for registration and exchange of data?
- To what extent should Danish laws be modified according to the proposals for common EU-rules to be introduced after the EU-commission has presented its drafts for a directive on personal data?
- In order to evaluate these questions a Work Group of experts within the areas of edp, law, public administration and communication was established. Through cross-disciplinary discussions, the task was to shed light on the subject and formulate a series of proposals which could be presented in a report and form the basis for discussions amongst politicians, relevant organisations and in a wider context -the public. The group has not evaluated all existing Danish legislation on registers, but has limited its efforts to subjects of own choice.

The Basis of Values

Edp - registration is not only a technological landmark, it is a phenomenon which deeply influences the structure of the society and the life of the individual. Thus, some regulation in the area is necessary.

Laws regarding registers should, for example, ensure the individual's right to privacy, which has been recognized as a human right - embodied in the European Human Rights Convention of 1950. The legislation can be looked upon as a defence against the access to (and also including possible infringements of) private matters, which the edp-technology has made possible.

Before embarking on a discussion of principles for registration one must take bearing of those norms which are to determine steering and course. One must plot ethical, social and personal values on the map. Only then is it possible to navigate between the emerging functional and principle considerations.

The Work Group has not been founded on a common basis of values, but has agreed to cite those values which the legal- and the edp-experts have formulated.

Mads Bryde Andersen:

-A complicated society unfolds itself by means of information. Information, given by the individual in interaction with others or to an undetermined circle of people should, as a starting point, be registrable and communicable - regardless of whether or not the communication takes place in the original form of the information (which rarely is seen), in an adapted form or as pieces in a mosaic.

If a person voluntarily transfers confidential or strictly private personal information- to single individuals, these "others" should consider the limitations which originally were set by the person in question, in the passing-on of information. With regard to such information the regulation of registers should to a great extent be unfolded under the market mechanisms or - by using legal language - be developed in accordance with set agreements. Special rules may however be needed.

If confident and purely private information is acquired by external pressure (this is practically important only for public authorities) there should be set limitations in the access to further transferral of information. The register legislation should in this respect be developed in close relationship with rules about professional silence.

Oluf Jørgensen:

-Public authorities and businesses make use of personal data in many ways, as for example for management and control. New technologies give possibilities for an efficient handling of electronic data which creates new forms of steering and control. In a democracy, legislative rules should ensure that not only technological possibilities govern the development. The important political question is: who should govern and control the society and how?

Protection of personal integrity is the most important aspect in the working out of legislation on personal data - other aspects are more easily taken into consideration. Citizens must be protected against the well intentioned guardianship of the authorities and against commercial business interests. The citizen's interests in the control of data and data processing are at least as important as the interests of different businesses and authorities. The individual citizen should be ensured possibilities for controlling his own situation, including registration and use of data relating to his/her own private matters.

Steffen Stripp:

-Personal data is a part of a person - in the same way as the body is a part. Therefore personal data belongs to the person.

It is a part of life to communicate with each other and be part of a society. The worst punishment is isolation. Protection of personal data is a human right and data protection

legislation deals with regulations in handing-over personal data. In a number of relations we hand-over information informally with the implied expectation of the intended handling of that information. In other relations, for example in dealing with the power of the state, information is given by external pressure. The essential notions are purpose, acceptance and recognition of an "untouchable zone".

The development of edp- and communication-technology offers increasing possibilities for storing, combining and transferring large amounts of data. The need for maintaining a very high level of personal data protection is still present and necessary if personal integrity is to be maintained.

Jan Aagård:

Regulation of registers should reflect a balance between the considerations of :

- Personal integrity
- Society's needs regarding matters of public interest
- The private sector's needs with regard to business and private activity.

It may be assumed that economy and rationality per se reduces an excessive data collection and edp- activity, in the same way as it must be assumed that the public use is creditable. Disputes on such matters can be finally decided by the Data Surveillance Authority.

It is recognized that personal information can be a presumption for granting and receiving social service in an integrated society.

Similarly, it is recognized that personal information - to an unacceptable extent - may be used for control and profiling of an individual. Disputes on these matters can be finally decided by the Data Surveillance Authority.

As can be seen from the above contributions, different points of view have been presented in which the notions of purpose, principle, consideration and function have been differently balanced. However, during the assessment, a broad consensus has been achieved with regard to the proposals and formulations which have been included in this report.

"Fear of Registers"

As a rule, registration has a sensible purpose. If a person in private or public activity spends time and energy on registration of personal data, it has an obvious purpose for the person carrying out the registration. But this purpose is often unknown to the person who is being registered, which may give rise to uncertainty.

Legislation on protection of personal data is founded on a very uncertain knowledge of the public opinion. Are citizens in general insecure of registers? Is there an unspoken fear of registration, or is the fear more diffuse and directed towards, for example, an uncertainty about "what it may be used for"? No updated investigation exists which may give a clear picture of either the possible extent of the fear of registers or of its direction.

In the summer of 1993, an intense press debate arose when it became publicly known that medicine consumption in Funen had been registered with civil registration numbers and multi-programmed with other registers in order to estimate the individual consumption of medicine.", Register blunder", "Police state methods", etc. were some of the expressions used against the researchers who were in the process of mapping the side effects of the medicine consumption. In the heat of the situation it was completely overlooked that the researchers were provided with all the necessary official approvals, and had been taken aback by the latent fear of registers in the population and the media.

In which situation does the fear of registers emerge? Is it created by the media or, is it built on substantial risks?

Presumably, it varies according to the actual situation. Some car-owners may not like to be enlisted in a register of the Danish car park. But that feeling may change if the register is used to refund the overcharge of fees for license plates.

The most substantial fear of registers seems to be directed towards the risk for societal control and surveillance of, the individual e.g. -What has become of my personal data? What do the police know about me? -How am I presented in the combined police index-register? - Could my telephone conversations be traced? -Does my case-officer know what I have told the doctor? -Can the tax authorities control everything? -Am I registered by the secret services or by their helpers? -Is the information on me correct?

Only few and relatively limited investigations have been carried out in this field. In 1987 an AIM-assessment (a consumer index assessment) for the Danish Board of Technology, disclosed a common fear of registers, per se. A similar result was found in 1991 in a so-called SENSOR-assessment for the newspaper "Jyllands Posten" concerning multiprogrammed registers. As there are no other Danish assessments in this area there is a need for further research in the field.

As a starting point, the Work Group assumes that the fear of registers in the later years has become less diffuse and more specific. Very few citizens have demanded access to registered information. In the municipality of Copenhagen approximately 100 persons per year have demanded access to their own registered information. In a middle sized provincial town approximately 20 persons have demanded access.

Taking today's mass distribution of edp-technology into consideration - especially the personal computers in professional and private life - the edp-technology has soon become public property. The irrational fear of the media and its possibilities has changed into a more factual kind of knowledge. However, although the common undirected fear of registration may decrease, this does not apply for the need for protecting sensitive, personal data.

The Edp-development

In 1976 approximately ten public authority registers containing personal information were in existence. Today, according to the Data Surveillance Authority, 3000 registers are in existence. The number of individuals listed in each register is not known.

In the private field, the Data Surveillance Authority has listed approximately 4000 registers. The actual number is much higher and new registers are constantly emerging.

Although the actual number is not known it has been estimated that more than half a million private registers may exist. But this is based on speculation, real investigations would strengthen the debate.

Together with the increase of registers, a remarkable technological development has taken place, including the market for personal computers. Still smaller computers have emerged with increasing capacities.

Edp-experts estimate that all Danish citizens in a few years time will receive a small plastic card, a so-called citizen card, which will contain all the civil information, which the public authorities may give out.

Edp in the Public Sector

The public administration (i.e. the case officer) decides when a case is sufficiently clear for a decision to be made. By means of edp-technology it can be done faster and cheaper than ever before. This can be considered a purely technical /economic improvement in the processing of the case.

But the edp-technology opens up for quite new possibilities. Via multi-programming of registers, the authorities can obtain insight into the conditions of the individual citizen even after the case has been closed. An insight which was previously impossible to obtain.

In 1985, for example, the Danish Broadcasting License Register was multi-programmed with addresses from the Building- and Residence Register with the purpose of disclosing licence-

dodgers.

In 1990 the Danish Parliament passed a bill which allows multi-programming of economic registers in order to control payment for public support, such as welfare payments, economic aid, pensions, etc.

Technically, it is possible to perform multi-programming on large public and/or semiprivate edp-systems and as such increase the efficiency of the social services and control of the citizens.

In the future, decision-oriented edp-systems in which manual input is minimized are expected to become widely used. Such systems are already in use within the tax administration.

The question is whether technical ability should govern the development, or whether rules of law and political decisions should set up the limits.

The Legislation

The Danish Laws of Registers, concerning private and public authorities' registers, came into force per January 1, 1979. These two laws have later been corrected and implemented - on April 1, 1988 (the private registers) and September 1, 1991 (the public registers).

Furthermore, rules about personal data have been introduced into several laws in specific fields: credit-cards, right to access to health information, registration, the databases of the mass media, etc.

The law about the public authorities' registers concerns, as a starting point, only edp-registers containing personal information. The law on private registers however, also concerns registers which are maintained with the help of pencils, ball pens, type writers, videos, etc. which is of interest if private or economic information or other personal relationships are involved, or in personal relationships which it would be reasonable to keep as private information. This law is not limited to personal information, but concerns registers covering institutions, associations, businesses, etc. Here, special rules are made for credit information agencies, databases of the medias, registers concerning telephone numbers and address services as well as mail inserting -agencies.

The citizens have a right to access to the public authorities' registers. In private registers the same applies, but only for edp registers. Still, the new law provides the right of access to health information at authorised private clinics, irrespective of whether or not the information is stored on a edp-system.

The laws about public and private registers include all types of personal information. Both

laws require as a minimum that the registration be a natural part of the business, and both yield greater protection for information concerning "strictly private matters" - ie.:

"information concerning race, religion, colour of the skin, political and sexual affiliations and punishable matters including information on health and essential social problems, misuse of stimulants and the like".

The rules for establishing registers are considerably more relaxed for private registers. In return, the rules for registration and passing-on of information under the category "strictly private matters" appear far more restricted. The civil registration number is here considered as "strictly private matters".

The Data Surveillance Authority which enforces these laws must, in advance, perform an evaluation of the specific guidelines before a register can be established. Furthermore, the Data Surveillance Authority performs spot inspections. In 1992 the Surveillance Authority performed 21 inspections in the public sector and 22 in the private sector.

The rapid development of the edp-technology in the society as a whole, creates a need for discussing changes of the legislation. Soon after the changes enacted in September 1991, the politicians predicted that the Danish laws would need to be revised again.. As stated by the Minister of Justice in the remarks to the bill, "there may be a need within the coming year for a more radical reform of the legislation for registers".

Proposition from the EU

It has been known for quite a long time that the Danish legislators are expecting a proposition from the EU.

The dissemination of edp-technology and a closer cooperation in the EU makes it necessary for the particular countries to make a decisive choice when it comes to legislation regarding edp-based registers. A balance between two opposite considerations must be found between the citizen (personal integrity) on the one hand, versus on the other, the society (an effective administration and control) and a free market (free mobility of goods)

The government of Denmark and the Danish Parliament are in the near future to take a position on a proposition from the EU-Commission about a proposal to an EU directive which builds on the principle of free mobility of data information within the EU. In September 1992, the commission presented a package of proposals to which the European Parliament, in turn, suggested several changes before the second proposal was made public by the Commission, in October 1992.

The final draft is not yet available. There are two leading ideas in the proposal. Firstly, a wish to protect the personal rights (the sanctity of private life). And secondly, to avoid trade barriers as a consequence of diverse rules for protection. The EU has therefore asked for a harmonization of the rules for protection of personal information.

The European Council Convention

Denmark has joined the international treaties covering this field, first and foremost the European Council Personal Data Convention which includes six additional supplements and which is considered the internationally leading treaty. The supplements are written as recommendations which are not legally binding for the Convention.

Article 6 of the European Council Personal Data Convention states that strictly personal information has to be protected by a special law in the national legislation. The Convention yields a minimum of protection for personal information. The individual countries can decide to tighten up the control of personal data information.

If a free data transmission is to occur across the borders, the relevant countries must have a uniform protection of personal data, so already here exists a problem. Five countries in the EU have not ratified the European Personal Data Convention of the countries Belgium, Greece and Italy - have no national legislation on protection of personal data.

No to the EU Rules

The Register Work Group under the Danish Board of Technology does not regard the proposed general EU rules useful for a regulation of the area. In practice, the proposal would cause great problems because the starting points for the individual countries are very different. Data protection ought, as a rule, to be kept a national matter in agreement with the principle of proximity.

There are at least two areas of special interests for a general EU-regulation. One area comprises police matters - in practice as expressed by the so-called Schengen Agreement. It is based on the creation of a common police register in Strasbourg "for communication of information with the purpose of keeping the public order and security including the security of the state, and to ease the application of the rules of this convention regarding travelling on common territory". The idea is that the opening of the borders between the EU countries should be met with a more effective internal control for the whole EU community. Denmark has not yet joined this cooperation.

The other area comprises development of the inner market which, in turn, will increase the volume of data exchange in all business areas. If defined areas show certain needs for special

EU rules in the form of supra-national control, such rules could be made especially for this particular purpose (credit information, marketing, address services bureau, edp-services, service, etc.)

But the general regulation should be developed according to cultural and administrative traditions in the individual countries.

In the following the Register Work Group will therefore focus on some proposed reforms in Danish edp legislation.

New Danish Laws

Today the public and private registers are governed by individual laws. This differentiation is artificial. The boundaries between the public and private is fluctuating, and there appears to be the same need for protection irrespective of in which framework the registration takes place (for example, insurance companies/hospitals).

In contrast, there exists a need for a two-way regulation. The Register Work Group proposes that the register legislation - in concert with the European Council, Convention be gathered under a general law which includes the relevant special rules.

The general law regarding protection of personal data should establish a number of common principles governing the right to access to registers, and how different types of personal information can be registered - irrespective of which connection the registration may have. This general law ought, at least, to obey the European Personal Data Council Convention. Furthermore, special rules for different societal fields ought to be made stating, in more precise terms, how the registration here can take place.

The advantage by using this legislative technique is that the lawmaker will achieve a greater overview of the consequences involved in passing these laws. In special areas another advantage is obtained as the lawmakers are forced to make their position clear regarding what kind of information should be governed by the limitations specified in the register laws - or the opposite, when a specific legislation has been made.

The general law on personal data should include both manually and edp-registered information. Because as modern techniques for scanning etc. are further developed, it becomes increasingly more difficult to define what is manually based and what is edpbased. Furthermore, the fundamental needs for personal protection are the same. Conversely a distinction between paper and edp may tempt the person in charge of the register to try to circumvent the rules by for example noting the information on paper in order to avoid the need to request registration.

By regulating particular areas, the purpose of registration can be precisely defined. Depending on the particular conditions, one can distinguish between collection, registration, application and passing on personal information. The handling of personal data must take place according to a formal procedure on a predefined level of security, and with a predefined procedure for deleting the information. The law should intensify the security measures with regard to confidentiality, possibilities for misuse and unauthorized persons knowledge of the information.

In connection with its convention on data protection - The European Community has pointed out areas which have a need for such special rules. These areas include for example, research and statistics, direct marketing, the social sector, the police, the labour market as well as companies who commercialize personal information, like address services and credit information services. Within the public sector, the introduction of a special legislative regulation in selected areas, will make it possible to limit or abolish the system comprised of previously criticized system of directives.

The Information Must be Differentiated

The final draft of the law ought to differentiate between three types of personal information:

- 1) common (name, address, telephone number and other information which are publicly available)
- 2) confidential (tax, credit card, statement of account including allotment of public support)
- 3) strictly private (health, political and religious matters etc.)

The registration of general information should be legal. There are no reasonable grounds for regulating and controlling the registration of information regarding, for example, owners of camping sites, employees in a workplace, pupils, car owners, etc. Today, the edp-technology is so disseminated, and is recognized that a legal registration will hardly arouse anxiety or uncertainty.

The confidential information is to be protected via general rules and special rules when need be. The attention should focus on the protection of strictly private matters. The information should, as a main rule, be given by the particular person him/herself, or acquired after consent and only when deemed necessary for the particular activity. Furthermore, the information should only be used to the specific purpose it has been collected for.

Today a centralized collection of strictly private information takes place, presumably without

the knowledge of the persons in question. This is a fact for several registers within the section of health - the Central Register for Abortions, the Central Register for Psychiatry, the Register for Malformation of Newborns, etc. Rigorous rules must apply for the use and passing-on of such information. Here, specific safety regulations must be defined.

A New Principle

Instead of allowing the principle that all registration is illegal unless permitted, one could introduce the opposite principle in the field of common information: Registration is permitted unless prohibited.

The Register Work Group has discussed the possible implications of this new principle by applying it in several specific but fictive situations:

1. Should it be legal for a group like the Hell's Angels, for example, to register the names and addresses of policemen?
- 2) Can individuals or groups register names and addresses of people who have expressed themselves as supporters for Zionist points of view?
- 3) Can a large amount of non-confidential information be registered and handled in a way that discloses a detailed knowledge of a single person's everyday life, for example via his shopping habits?

The Register Work Group's response can be expressed as follows, in case the new principle was valid:

Ad 1: Yes, under the presumption that the registration, as such, is legal. If so, a group cannot separately be denied the right to register non-confidential information. But if the registration takes place together with the advancement of threats and thereby having the character of preparations for an action, it will already be illegal (according to the Criminal Code regarding threats combined with attempts at breaking the law).

Ad 2: Here the same applies. If the registration appeared to be in preparation of a real criminal act, for example support to a foreign state intelligence service, the registration would be illegal.

Ad 3: The example shows why one ought to differentiate between collection, registration, use and passing on of data. The important point is what kind of purpose the combination of data serves. It can also be relevant to know whether the registrant has approved the act.

Admission to Own Data

Many banks and credit institutions make it possible for the individuals to seek information about his/her own account via the telephone. A natural step along these lines would be that the single citizen - under a high degree of security - be given electronic access to his/her own personal data in public and private registers.

The single citizen's access to his/her own personal information is decisive for control and improvement of the quality of the collected data.

New Rules for Multi-Programming

In several instances different public registers have been multi-programmed for the purpose of increasing control. Large groups of recipients of public support have been cross-checked in order to ensure that nobody received too much assistance in social security, unemployment benefits, housing support etc.

It is worth noting that there is a great difference between passing on single information on a concrete suspicion as compared to multi-programming of registers in order to find possible sinners, but this is not the way the laws apply. The law regarding the public registers has the same criteria for passing on single information as it does for combination of registers involving mass information. Here one has to differentiate according to the character of the information.

- a) If it concerns general information, it is unproblematic to perform multi-programming of the registers in order to, for example, up-date information on addresses.**
- b) Multi-programming of confidential information for background checks must be governed by special rules. Here, one must take into consideration whether the registered persons have been warned specifically about this possibility before they handed over the information.**
- c) Multi-programming of strictly private register information for the purpose of background checks ought, as the main rule, to be illegal.**

Independent and Active Supervision

It is as a part of the requests for data protection -which include, for example, The European Council - that an independent authority exists which can supervise the registration of personal data, as well as act as an authority for complaints.

In Denmark the Data Surveillance Authority carries out this task under the responsibility of the Danish Register Council whose members are appointed by the Ministry of Justice. The director of the Data Surveillance Authority is likewise appointed by the Ministry of Justice. The Data Surveillance Authority and the Register Council are simultaneously advisory, supervisory, instances for complaints and a part of the administrative apparatus which they are to supervise. In practice this implies a weakening of their independence.

One step towards increasing the feeling of security would be to introduce changes which would strengthen the independence of both - the Register Council and the Data Surveillance Authority - with regard to the supervision of the government and the Ministry of Justice.

The resources and activities of the Data Surveillance Authority ought to be expanded in order to undertake investigations on its own about personal data, and to build up knowledge in this field which, in turn, would be very useful for a more qualified and active participation in the public debate.