Denmark adapts data laws for the information society

In Denmark, as in other EU-member states, there have been few statutory changes in data protection law in recent years, as the European Union directive on data protection was awaited. In this report, Professor Dr. Peter Blume, Director, Institute of Legal Science, University of Copenhagen, examines the recent amendments to the Danish data protection laws to adapt the law to the challenges of the information society.

To make substantial changes in current law has little meaning, as the EU directive will make a comprehensive statutory reform necessary. The years taken to come to an agreement on the directive creates problems, not least of which is that the developing information society makes it expedient to consider whether amendments to current acts should be implemented. However, uncertainty surrounding future EU rules has not meant a total standstill in Danish law. Section 2 of this report outlines general plans for the information society. How the directive will be implemented is described in Section 4.

1. Communication of public debts

On December 13th, Denmark's Parliament passed a bill which among other things amended the Public Registers Act. The new Act (1093 of 21st December 1994), inserts a new chapter (5A) in the Public Registers Act making it possible for public authorities to report debts to private credit reference agencies. This had not previously been possible as the data is confidential. The practical consequence was that debtors were inclined to pay private debts before public ones. If there were only public debts there would be no record in credit reference agencies. This situation has been seen as one of the reasons for the huge debts to public authorities.

The new rules are intended to contribute to a reduction of public debt. The regulations take into account that communication of such data from the public to the private sector is a delicate matter and accordingly should only take place when clear conditions are fulfilled.

Section 20a states that information on debts to public authorities may be communicated to credit reference agencies. However, sensitive data cannot be communicated which means that the reason for the debt must not be disclosed. The communication of confidential data does not mean that the data has in any other respect lost its confidential character. In any case, customers of a credit rating agency are obliged by contract to handle received information confidentially and must not communicate it to third parties.

Section 20b contains more details of regulations concerning circumstances in which debts may be reported. The new rules apply only if other statutory rules do not exist. Only due debts of at least Dkr25,000 (£2,800) may be reported if a payment agreement has not been reached. The reason for this rule is that debts to public authorities often do not have the same voluntary background as private debt, and small debts should accordingly not be reported.

Subsection 2 states additional conditions that must be fulfilled before reporting of such debts may take place. The conditions mentioned in the following are alternatives:

1. Debts that can be paid by execution of a distraint order after two collection letters have been sent. This condition will apply to taxes, for example.
2. Situations where seizure has been made or attempted.
3. Where the debt is stated in a final court decision.
4. When the debtor has recognised, in writing, the existence of the due debt.

Section 20c states that before a debt is reported, the authority has to inform the debtor, in writing, that this will take place and the actual reporting cannot take place until four weeks after such information has been given. This section also describes what the information must contain. It must include the data which will be reported, to which agency, and at what time, and that reporting will not take place if the debt is paid or a payment settlement is reached.

Section 20d states that the responsible minister, after consultation with the Data Protection Agency, may issue administrative rules on the procedure or determine other conditions than those outlined in section 20b.

These rules illustrate how important data protection is considered in Danish law. Although the rules fill a major gap in Danish legislation and will improve the public economy, they also ensure that not only is the reporting of debt more accurate, but that there is a good possibility of debtors avoiding such reporting. For these reasons it is understandable that the new rules have not met with any criticism.

2. Data matching

As part of the political agreement on the state budget for 1995, several amendments to tax legislation were passed (Act no. 1113, Dec. 21st 1994). A new rule (Section 7c) was inserted in the Tax Control Act (consolidated no. 555, June 24th 1994). This rule increases the possibility of data matching from public files so that payments are more accurate, and public expenses thereby reduced. International experience, however, demonstrates that this is seldom the result in practice (PL&B Dec. 1994, p. 11).

The new rule requires that employers report employees in receipt of taxable income to the state tax authorities. This reporting is on a monthly basis, using a personal identity number (PIN). Also, unemployment funds may be required to regularly report the PIN of recipients of maintenance allowances. This data may be electronically transferred to state and local government authorities and to unemployment funds to control the accuracy of payments. The recipients of such data are permitted to match the data with their existing files.

Level of surveillance increased

It is, in particular, the current and constant reporting that is new. This innovation has been enthusiastically welcomed by representatives of local government who believe that their costs will be substantially reduced. The new rule increases the level of surveillance and must, from a data protection perspective, be viewed with considerable caution. Although matching must conform with the general rules in the Public Registers Act, this new rule is disturbing.

3. Info-society year 2000

In October 1994, The Research Ministry published a report, *Info-society year 2000*, outlining how Denmark can adjust to the developing information society. The report was followed in March 1995 by an action plan issued by the Government and later debated in Parliament. This plan will be updated annually. The plan and the report contain several proposals with data protection implications and view data protection as a basic obstacle to efficient information technology implementation.

The basic aim of the report and action plan is to outline how the public sector should be reorganised to take full advantage of modern information technology. Although the private sector is seen as the main player in the development of the information society, state and local government have important functions. The report (p.33) states that: "Information which has already been submitted by citizens and companies to a public institution, and which can be transferred electronically, shall not be requested by another public institution again." It is clear that such a principle has important data protection implications as it presupposes that data may be communicated freely between public authorities and that these become one big data community.

The result of this principle is upheld in the action plan but is somewhat modified as it is stated that transfer of data may be made dependent on data subject consent.

The aim of data protection legislation is to make "it possible to register, combine and use data for all legal and administrative purposes without bureaucratic procedures" (report p 45). The current legislation must accordingly be reviewed and the new rules should concern personal information, not files. Current demands for registration or statutory reporting to the Data Protection Agency (Registertilsynet) should be removed. The new act should concern personal information regardless of whether it is processed manually or electronically. Further, restrictive rules should only apply to sensitive data. Finally, there should be improved possibilities for data matching, and a comprehensive reform to reduce restrictions on public administration. The connection between these far-reaching ideas and the EU directive is described in Section Four.

Citizen's Card proposed

There is also a proposal for an electronic citizen's card with a PIN code and picture to be used for positive identification of the individual citizen in his contacts with public authorities. The card would contain only a personal identity number, no other personal data, and would be

voluntary and regulated by a special Act. The advantage of such a card is that citizens will only have to use one identification card when dealing with public authorities instead of many cards which would be a likely alternative. It is proposed that the card can be used in connection with electronic self-service administration systems. The card can be used to gain access to personal data and furthermore to give consent to the use of personal data by a public authority. It is clear that a citizen's card, although not an identity card, has serious implications for privacy and a heated public debate can be expected when this proposal is laid before Parliament.

Health Network

Another interesting plan is to develop a nationwide health network for the interchange of information. The purpose is that electronic medical data concerning individual patients would be communicated both to hospitals and to general practitioners and other doctors in the private sector. The full development of such a network presupposes a national standard for electronic patient case files and clinical databases which can contain complex forms of information.

Although the first steps towards such a network has been taken in the MEDCOM project, a fully established health network is first expected after the year 2000. Clearly, this development will lead to communication of very sensitive personal data between the public and private sectors and presupposes strict and efficient security measures. From a data protection perspective, it will be necessary to follow these plans carefully to ensure that infringements of privacy are prevented.

4. Preparing the new legislation

The action plan proposes that before the summer of 1995 the Ministry of Justice set up a committee to prepare new data protection legislation. The committee is to present its report before the end of 1996. Before the final adoption of the EU directive, consideration will begin on the extent to which the ideas described in Section 3 are in accordance with the directive, and how it is to be implemented in Danish law. It is estimated that new legislation must come into force at the latest by 1st January 1999. As the directive will present a huge and complex legislative task, it is recommended that detailed consideration starts early and, as the common position is now known, it is rational to let the work commence now.

The report *Info-society 2000* has been published in an English version. It can be ordered from Schultz' bookstore, Herstedvang 10-12, DK-2620 Albertslund, Denmark. Phone: +(45) 4363 2300 (price: Dkr. 90 - approx. £10).

This report was written by Professor Dr. Peter Blume, Director, Institute of Legal Science, University of Copenhagen.