DENMARKS'S DPA REGULATES PRIVATE SECTOR MATCHING AND RELIGIOUS DATA

DPA regulates private sector matching

Over the past year, the Registertilsynet, the Data Protection Authority (DPA), has considered a number of cases regarding *matching of files held by private companies.* The Act prohibits matching files. The DPA may, however, allow such matching under certain conditions. An analysis of several matching authorizations for companies shows that the common conditions are that:

1. *the controller* responsible for the matching *must be named;*
2. the matching must be in the clear *interests of the registered data subjects;*
3. the *location* of the matching operation must be stated;
4. the *categories of data subjects* involved in the matching must be stated;
5. the *types of data* covered by the DPA's authorization must be stated;
6. the *data subjects* whose data is being matched *must be informed in advance;*
7. the *purpose of the data match and the way in which the matched data will be used* must be stated. In principle, there could be a problem with companies which carry out a data match for one purpose but then want to use the data for a related purpose. Such a change of use should be referred to the DPA but, in practice, no company has yet done so;
8. data subjects must retain a *right of access* to data on themselves;
9. data processed in the matching must be *accurate and not misleading.* If errors are discovered, they must be corrected as soon as possible;
10. the DPA must be informed of any *changes in the company* relevant to the matching; and
11. further conditions may be needed for data matching involving *sensitive data,* although there have been, so far, no such cases.

Some of the matching cases resulted from large financial groups' plans to offer their customers financial services consisting of products from different companies under the *same holding company* and to match the files of the customers in these companies.

Other cases have illustrated an increasing trend among *unrelated private companies* wishing to exchange data about customers for the purpose of marketing, either through the passing on of data or through file matching.

DPA orders Jehovah's Witnesses to destroy sensitive data

In a case of major interest to the public and the press, the Jehovah's Witnesses in Denmark kept extensive files storing large amounts of data of a highly sensitive nature about former members of the religious community who had been expelled or had left the community voluntarily or against whom disciplinary measures had been taken.

In mid-September, 1992, the DPA ordered the Jehovah's Witnesses to erase all sensitive data about former members and current members against whom disciplinary measures had been taken. They were permitted to retain factual data simply stating that a member had left the community or that disciplinary measures had been taken. The Jehovah's Witnesses were given a deadline in November 1992 to carry through this order and they have now done so.

Government aims to increase efficiency by abandoning purpose limitation

In the spring of 1992, the Ministry of Finance issued a report on the *Efficient Use of Information Technology in Government Administration.* Due to financial problems plus a high tax level in Denmark, this report put

emphasis on efficiency, and the Ministry suggested amendments to the present data protection legislation, without specifying such changes. Its main idea was that all government agencies should be able to re-use basic data once collected without regard to the purpose for which this data was originally collected.

Up to now, there has been no discussion of the report in Parliament. The Ministry of Justice has suggested that the proposals in this report should be examined together with the revised EC draft directive.

Public sector procedures simplified

Amendments to the Public Authorities' Registers Act entered into force on September 1st 1991. Their aim was to simplify the procedure for the establishment of certain types of public sector computerized files which were considered to involve no particular privacy risk. In this way, a *notification* system has been set up, as opposed to a system of *approval,* but only in the case of basic, minor files.

Before these amendments, the Act had prescribed that a set of detailed directions had to be given for every computerized file containing personal data. Although the law provided for specific types of files to be exempted from this requirement, every file still needed the approval of the responsible political authority before a public authority could legally establish a new system or file containing personal data.

The amendment to the Act allows local authorities and government administrations to establish files without issuing a set of directions and without political approval when the file in question does not contain data considered to be confidential, or when only identification data (including the PIN number) and data concerning payments relating to a public authority are stored. Administrations must, however, notify the DPA of the establishment of all such files. The DPA has the power to decide in specific cases that a set of directions shall be issued.

Furthermore, the Minister of Justice has laid down rules to the effect that certain *types* of files are exempted from the notification requirement, for example, environmental systems, personnel administration systems, library systems. It is clearly stated in the Act that these types of files must not contain data of a sensitive nature, such as health or criminal data.

The amendments concern only the formal procedure on the setting up of certain types of files. The files are not exempted from other provisions in the Act, and the level of security required has not been changed.

Does the notification system work?

The notification system has now been in force for one and a half years and the DPA has gained some experience. A great deal of care and resources went into the drafting of instructions for the new rules and the production of two notification forms to ensure that incoming forms are standardised.

By September 1st 1992, the DPA had received approximately 1,500 notifications of files under the new system. However, fewer than 40% of all local councils (99 out of 275) had, at that stage, notified any files at all. This figure should be compared with the fact that during the first 13 years of data protection legislation in Denmark the DPA received more than 2,500 sets of notifications for files set up in the public sector. It is difficult to give an exact explanation for this apparent sudden increase in the number of files in the public sector. Maybe it is due to an increased use of computers or merely perhaps to an easier formal procedure before setting up a file.

The DPA has in fact received a number of notification forms from which it appears that the file in question was set up before the notification system was even introduced. In several cases the DPA has asked the local council to stop the operation of specific files storing sensitive data until a set of directions has been approved.

Media information registers law proposed

In early 1992, a Commission was established by the Minister of Justice to publish a report and propose a draft law on *Media Information Registers*. The DPA's representative on the Commission was its Head of Department, Lotte Jorgensen,

The draft law proposes regulation of media electronic information registers generally accessible to the public and of information registers used solely for journalistic purposes.

The Commission did not reach consensus on a number of key points. There were disagreements, for example, on:

- the definition of *media*, defining who can legally keep information registers for journalistic purposes
- whether or not publication of an article in itself is sufficient proof of media status to justify legal protection for the personal data contained in any related database
- rights of access by the data subject.

The Report has been submitted to the Minister of Justice, who is responsible for presenting a bill to Parliament.

The Board of the DPA was asked by the Minister of Justice to give its opinion on the report. The Board shares the view that some regulation is necessary, and has pointed out that the majority's draft falls short on a number of basic data protection principles. Thus, the Board has made suggestions for tighter regulation of the media. Subsequently, in March 1993, the Minister of Justice made a proposal for a Media Information Registers Act.

Use of health data for other purposes

There has been much public debate in Denmark on the storage, use and transfer of health data, both for administrative and scientific use. A leading issue is consent from individuals whose data, already stored for other purposes, is used for scientific research.

Parliament has passed a minor, but important amendment to the *Medical Doctors' Act*. A doctor now has a duty to inform patients about their state of health and patients have a right to *receive information* and give their *consent* to further treatment. This amendment includes the patient's right to make a *life will* i.e. any person may express the wish for ending life-prolonging treatment in a situation where the testator is inevitably dying.

In June 1992, Parliament passed an Act setting up a system of *scientific ethical committees*, with the task of approving biomedical research in general.

Genetic testing bill soon

In April 1992 the Minister of Labour introduced a bill to the legislature concerning the use of genetic testing in connection with *recruitment, pension settlements and insurance.* The bill was not passed by the end of session but it is expected to be reintroduced this year.

DPA takes public interest archiving decisions

In May 1992 the legislature adopted a *Public Archives Act* to raise awareness of the public archives' role and to provide optimum conditions for research in the public interest.

The Act states that all *governmental files*, no longer being used and storing data electronically as the key to the manual case records, should be handed over to the central governmental archiving institution. Other governmental files should be archived when considered necessary for the carrying out of scientific or statistical investigation of paramount importance to society at large. In these cases, the DPA takes its decision after the central government archiving institution gives its view. The archives are generally inaccessible to the public for a period of 80 years.

Privacy Laws & Business gratefully acknowledges the help of Lotte Jorgensen, Head of Department at the Registertilsynet, Denmark's DPA, in the preparation of this report. She also is the current President of the European Community's Council of Ministers' Data Protection Working Party.