THE ROLE OF THE COUNCIL OF EUROPE IN DATA PROTECTION

The Council of Europe, the EEC and the OECD

The Council of Europe, based in Strasbourg, is an intergovernmental organization established after the second world war for the purpose of achieving greater unity of the European democratic countries. It includes all the EEC countries, the Scandinavian countries (Finland is an observer but has recently applied for membership), Switzerland, Austria, Turkey, Cyprus and Malta. Its decisions are influenced by a Parliamentary Assembly and taken by a Committee of Ministers.

The Council of Europe's approach is legal, social and educational. One of its major achievements was the European Convention on Human Rights, concluded in 1950, which established a Commission and a Court of Human Rights.

The Council of Europe should be distinguished from:

* The European Economic Community, the EEC, which has a Council of Ministers, as its top decision-making body, a Commission, based in Brussels with some supra-national authority, a European Court of Justice, based in Luxembourg, and the European Parliament based mainly in Strasbourg.

* The Organization of Economic Cooperation and Development, the Paris-based OECD has in addition to the countries which are members of the Council of Europe, Australia, Canada, Japan, New Zealand and the USA.

All three organizations have an interest in data protection.

The Background to the Council of Europe Convention on Data Protection

At the end of the 1960's, the Council of Europe's Parliamentary Assembly asked the Committee of Ministers whether the Convention of Human Rights and national law gave sufficient protection to the right of privacy in view of developments in information processing. The Committee of Ministers concluded that there were several problems to be resolved:

1. The European Convention on Human Rights covers in Article 8, in general terms the right to a private life, but does not apply to the private sector.

2. The right to a private life would not necessarily include all personal data, and so there was a question whether a large proportion of data would be sufficiently safeguarded.

3. The right of access to data on oneself was not covered by the concept of the right to privacy as expressed in Article 8.

In short, the European Convention had a defensive approach to privacy and more positive action was necessary.

As a result, at the beginning of the 1970's a Committee of Experts was established which prepared two recommendations with basic principles for the protection of privacy regarding electronic data banks. These

recommendations were agreed in 1973 and 1974, one covering the private sector and the other covering the public sector. The recommendations covered the principles, like data collection, storage, use, rights of access and correction, which in 1980 were incorporated in the Council of Europe Convention on Data Protection.

Meanwhile, the German Land (regional government) of Hesse had passed the world's first data protection law in 1970, followed by Sweden in 1973, and several others in the next few years. These laws led in the second half of the seventies to the preparation of the Council of Europe Convention on Data Protection for three major reasons:

1. Several national data protection laws included provisions on transborder data flows restricting the export of data so that privacy would be protected. This permission or licensing system threatened international cooperation and communication.

2. Although the national laws were inspired by the same basic principles, there were several differences in substance and procedure. This meant that as soon as there was a problem with international data processing there were serious problems of conflicts of law.

3. The human rights concept behind Article 8 of the Council of Europe Convention on Human Rights needed to be expanded to more fully cover name-linked data.

The Provisions of the Council of Europe Convention on Data Protection

The drafting of the Convention started in 1976 and was opened for signature on 28th January 1981. It covers the automated processing of personal data and contains four major elements:

1. The basic principles of data protection should be the basis of all national legislation and all countries ratifying the convention should take the necessary measures in its own law to give effect to these basic principles, at latest by the time of entry into force of the Convention.

2. Assuming that ratifying countries have laws which are similar in substance, there should not be any limitation on transborder data flows between ratifying countries. However, exceptions may be made, for example, medical data or data on racial origin.

3. Ratifying countries should offer each other mutual assistance. A data subject in one ratifying country wishing to gain access to a file on himself in another ratifying country may obtain the assistance of that country's data protection authority.

4. A Consultative Committee has been established to oversee the working of the Convention and to suggest improvements. So far, it has met once every two years, but now it is intended to meet more frequently.

Ratifying Countries

The Convention came into force on October 1st 1985 after five countries had ratified: Sweden, Norway, France, Germany and Spain. Since

then, Austria, Luxembourg and the UK have also ratified it. The next countries to ratify the Convention are expected to be Denmark, Ireland and the Netherlands.

Council of Europe Sectoral Recommendations

When the Convention had been concluded, the committee of experts turned its attention to sectoral recommendations as it considered that the general principles needed to be applied to specific sectors.

The first was on automated medical data banks in 1981. This contained an element of self-regulation, as it stated that each data bank should have its own regulations which should specify, for example: the purpose; the categories of information recorded; and the purposes for which the data is being used and so on, A through M. Clearly, in that early phase, self-regulation within the law was considered to some extent.

The second was on research and statistics in 1983. Here, the main points are:

* whenever possible research should be done on the basis of anonymous data. Obviously this is not always practicable, but data should be anonymised as soon as possible. Techniques for anonymization are indicated in the explanatory report.

* where data is collected from the data subject for scientific research, the data subject should give his informed and explicit consent and he should be free to withdraw his co-operation at any moment. If someone is not obliged under law to co-operate he should be informed of this fact.

* for statistics and scientific research, the principle of purpose limitation is very strict. This is illustrated by what I call the "iron triangle" of data protection concerning the purpose of storing data. The purpose has to be specified, it should be legitimate, and should be reflected in the data being collected and stored. The purpose sets the limits in terms of use. In the case of statistics and scientific research, any use beyond research and statistics is incompatible. That is the golden rule in this area.

* the Convention itself allows an exception to the right of access in the case of files for statistics and scientific research. The reason is that statistical data is arranged in such a way that it is extremely difficult to answer straight questions. For example, a data subject may come to the Central Bureau of Statistics and ask if there is any data on him. If there is an obligation in law to arrange the data in such a way that these questions can be answered readily it would be against the interests of privacy protection. The way in which these statistical offices handle their data is usually a very sound one. So the Convention allows for an exception to the right of access where there is no risk of encroachment on privacy and this principle is reflected in the recommendation.

The new element to the Council of Europe Recommendation on Direct Marketing is that there is an unconditional right of the data subject to refuse to allow data on him to be recorded on marketing lists, to refuse to allow its transfer to third parties, and indeed unconditionally to have such

data erased or removed. To a great extent, if you look at the text, use of personal data for direct marketing is accepted and allowed. In order to exercise the right to refuse permission for data to be recorded or transferred, one must have sufficient information at an early stage.

Two other recommendations have been accepted - social security and the police. In both cases, much of the data is sensitive. We consider it a major accomplishment that it was possible even to agree on the text setting the rules for data protection in the field of police records.

The next recommendation on employment records is due to be approved by the Committee of Ministers in early 1989 (see p.2).

Then there is a working party dealing with financial services, especially new technology like chip cards and electronic funds transfer at the point of sale.

There is another working party dealing with the intersections between freedom of information and privacy, access law and data protection law. The two areas of law create some problems in practice. In France where there are two different laws there are sometimes problems of who is authorised to do what. But the right to privacy sets limits on publicity, and the right of access may break up data protection. That is a problem. The meeting between publicity and privacy is a general problem but arises also in terms of archive law. In some cases, we have special public registries on personal status - like marriage, property, real estate - which present interconnecting problems.

We have had a working party on new technologies in general, apart from the banking sector, especially three types: telemetry - collecting of information from a distance, for example, gas and electricity meters, and especially, paid television data. We are more and more living in a wire-tapped house (to overstate things) and privacy problems deserve a close look; electronic mail; and interactive media, for example, videotex.

The result of that study has been put into a report which the Committee of Ministers has approved for publication very soon. It sums up the state of affairs in these three areas, highlights data protection problems and possible solutions and then a cross cutting section on the basic principles. Do they still stand? Yes, it concludes - they are basic and flexible enough to be interpreted in a meaningful way in these new contexts.

The Committee of Experts has had some discussion on extending the work on new technologies and focussing them on telecommunications. Also a working party is going to look at genetics. The scope of the subject is enormous and the variety of areas to which these basic principles apply is also extensive.

A very practical advantage of having this committee is that it is a meeting and market place of experts - lawyers and technicians - dealing with these matters for their governments and exchanging information and experience, looking for help and inspiration from other countries. We have had discussions on personal identification numbers, personal identifiers which from the very beginning until now raise anxiety among the general public. Finally, we are going to look at self-regulation at our next meeting.

On the legal status of recommendations, a recommendation can only recommend a certain course of action. - it is not legally binding. A convention goes through the following stages. It is first prepared by the Committee of Experts; is then accepted by the European Committee on Legal Cooperation which is basically again an intergovernmental committee; it then passes to the Committee of Ministers, approved; and then opened for signature. Every country signing the Convention accepts a moral obligation to work towards ratification. Ratification means that a country accepts to be legally bound by the Convention.

In the case of a recommendation, it undergoes the same course of preparation. The Committee of Ministers approves the recommendation which means that all countries voting in favour accept the recommendation as a source of inspiration. It is not binding in the strict legal sense but in practice, these principles are being used as a measuring stick for national legislation. It is my experience that often parliamentarians raise questions in the light of these recommendations.

A country having ratified the European Convention on data protection and then accepting a recommendation on police or direct marketing, is actually saying that it accepts that these general principles, which they endorse or consider to be binding, have to be interpreted a certain way. Therefore, in these countries, a recommendation has more authority, but strictly speaking is not legally binding.

If a ratifying country acts contrary to a Council of Europe Recommendation which it has accepted, major breaches are usually brought out at the diplomatic level by the Committee of Ministers which meets every month or so in Strasbourg. The Data Protection Convention does not have enforcement machinery. For those countries which have ratified the Council of Europe Convention on Human Rights, as far as Article 8 (the right to a private life) is concerned, the Court of Human Rights has on several occasions, in minority opinions, indicated a willingness to use the Convention on Data Protection as a source of inspiration for a dynamic interpretation of Article 8 itself. In the case of police files, the principles of the Data Protection Convention are being included within the scope of Article 8. Thus although a recommendation may be non-binding, it may become more binding because of Article 8 and its machinery. There are different possibilities. At some point, a recommendation may turn out to be binding.

The Data Protection Convention also has a Consultative Committee which although it does not have an enforcement role, may act as a lubricant in the operation of the Convention, especially in the field of transborder data flows.

This is an edited version of the address given by Peter Hustinx, Chairman of the Council of Europe's Committee of Experts on Data Protection at the Privacy Laws and Business Conference on October 19th 1988 in London.