FULL AGENDA FOR SWITZERLAND'S FEDERAL DATA PROTECTION OFFICE

Since our first issue in early 1987, we have reported on the slow progress of Switzerland's Data Protection Bill. However, the Federal Data Protection Office has been busy not only redrafting the general legislation and helping its passage through the legislature, (see page 11) but also giving advice to both the public and private sectors in several important areas. Dr Peter Muller, Head of The Data Protection Office at the Federal Justice Department, explains his department's wide-ranging activities.

Sectoral Legislation

The lengthy period which has been required for the development of a general law has led to the development of rules for specific sectors. So far, experience has been mixed. Such regulations frequently remain incomplete despite serious efforts, and they create contradictions in relation to a general data protection law, and traditional rules on secrecy. The danger is that the authorities responsible for the enforcement of the law on the processing on individual's data no longer know which rules apply.

In Switzerland, this problem is made worse due to the fact that the Confederation (Federal Government) and the cantons, are both competent in several areas (for example, social insurance, the law relating to foreigners and the army), and that the demarcation between federal law and canton law on data protection is difficult to draw.

State Trade in Data

The State often takes the role of both the protector and supplier of data, and it is sometimes very difficult to reconcile these activities. In Switzerland, these types of problems particularly apply to the Register of Companies and for the postal service, which provide mailing addresses as a service. In these two cases, the Federal Data Protection Office has with some success supported the principle that the State may make personal data available only with the consent of the person concerned. The exchange of information between the State and the private sector should not be forbidden according to the Federal Data Protection Office, but it should be limited according to the right of self-determination of the person concerned over data on him.

The Sanacard (Health Card)

The Federal Data Protection Office has been asked by the private sector for its view on the Sanacard project. Sanacard is a magnetic card, on which is registered an individual's identity, health data, address in case of emergency, address of doctor, information on health insurance, and other data. Doctors, pharmacists, hospital administrators and insurance company staff may read the card using special equipment, and may also add new data on the card.

After a thorough investigation the Federal Data Protection Office has

decided that such a card conforms to the principles of the Data Protection bill as long as the following conditions are fulfilled:

1) The person concerned should receive a new copy of the contents of the card when each change is made.

2) The person concerned must himself at all times have the right to wholly or partially delete any information on the card, and this principle also applies to sensitive data such as AIDS.

3) The different users of the Sanacard may have access only to the data which is necessary for them to do their work.

4) Only the identity of the individual may be communicated to the factory which makes the card. The health data may be supplied and added to the card only by medical personnel.

Revision of the Army's Automated Personnel Management System

This system with 1.2 million names is one of the most important data banks in the federal administration. A great number of federal and canton authorities are recorded on the system. Its use is ruled by a special detailed ordinance. In the course of this year, the Federal Data Protection Office has carefully examined whether the use of this data in practice accords with legally determined processing procedures.

The general impression is that the high standards have been achieved. However, it has been noticed that the way that access is authorised in practice does not match legal requirements in every respect. More services have access to the system than the legislator has envisaged. Furthermore, the accuracy of the data is not always sufficiently guaranteed. That results from the fact that much data, including sensitive information such as court judgements, are not updated frequently enough. Finally, it appears that the system documentation is not completely up-to-date, which makes the task of enforcing the law more difficult.

Changes to the management system which the military authorities themselves mainly support have received an equally favourable reception from the system's own data managers.

The Federal Data Protection Office is going to conduct a similar audit in all the other major systems within the Federal Administration.