SWITZERLAND ADOPTS A DATA PROTECTION ACT

On 19th June, 1992, Switzerland's two legislative chambers, the Conseil d'Etats and the Conseil National, approved a Data Protection Act. It will give individuals new rights in the public and private sectors and impose new duties on any person holding or processing personal automated or manual data relating to an identified or identifiable individual. There are some novel and specifically Swiss characteristics of the new law.

The most democratic aspect is that the new law will be subject to approval by a referendum if at least 50,000 Swiss citizens sign a petition requesting one within three months of the law being adopted by the legislature. Informed observers do not expect a referendum, in which case the law will probably enter into force on January 1st 1993.

Legislative History

The pace at which data protection legislation has been progressing in Switzerland has been much slower than in the other European countries which serve as major financial centres. This is largely because laws can generally only be passed if they receive the backing of the major unions and trade associations. Industry has however traditionally been critical of the introduction of data protection regulations.

Switzerland's first data protection bill was published in December 1983 but in 1984, after wide consultation, this bill was amended by the Justice Minister. The most interested organizations consulted were in favour of a data protection bill but considered that many points needed to be studied thoroughly. Subsequently, the Justice Ministry revised the text and the Federal Council (the Government) presented the legislature with a new bill on March 23rd 1988.

The bill was passed by the *Conseil d'Etats* chamber of the legislature in 1990. It was debated by the relevant committee of the directly elected *Conseil National*, the second chamber of the legislature, in March and April 1991. The *Conseil National's* plenary session approved an amended version of the bill on June 21st 1991. After differences of opinion between the the two chambers were resolved, the bill was adopted on June 19th 1992.

Main Provisions

The general principles of the law and the operational rules are binding on both the private sector and federal authorities. A number of security safeguards have been built in, such as the requirement to register certain types of data systems, and notification of file transfers abroad.

Physical and legal persons: A special feature of Swiss bill is that it protects and gives rights to both *physical persons* and *legal persons*. This means that it not only protects employers and employees, but international organizations, communes and companies as well. Under the Swiss constitution and Civil Code of 1907 a legal person also has a right to privacy and should, therefore, be able to defend himself against unlawful data collection. Public opinion demands that local governments and industrial concerns expose their activities to close public scrutiny. Company secrets are already protected by the Swiss Criminal Code.

Automated and manual data: The bill regulates *automated and manual data collection* in the same manner. During the preparation of this new law, it was discovered that a problem was posed not only by electronically collected information, but also by manually collected data. If, for instance, an employer keeps an illegal blacklist of union-organized workers, or a union maintains lists of strike breakers, then it makes absolutely no difference whether the list is computerized or kept in a filing cabinet. Similarly, if a firm divulges the addresses of its clients against their will, then it is irrelevant whether this is done on-line or by messenger.

Sensitive data: The new Swiss law contains provisions on *sensitive data* based on

the Council of Europe Convention on data protection. Sensitive data includes information on an individual's religious affiliation, ideological or political beliefs, and union activities, as well as his state of health, private life, racial origin or criminal record. Such data can now only be collected for a legitimate and specified purpose when there is an overriding interest of the data processor. A publisher, for instance, who wants to propagate a particular religion or creed, may ask his employees for details about their religious beliefs.

The data protection principles: The general principles apply to both *private data collectors and processors* as well as to the *federal authorities*. They are - with few exceptions - the same as those laid down by the Council of Europe Convention on Data Protection and by many other Data Protection Acts:

- Data may not be collected *by unlawful means*. A firm, for example, may not obtain information from a competitor under false pretences - by professing interest in a joint venture, for instance.
- Data must be *accurate*. A credit information company which has confused someone's identity and therefore given false information on that person may be liable to pay compensation.
- Data processing must be *relevant, adequate, not excessive, and not unfair*. A company may not conduct investigations into the private life of the manager of a rival firm in order to gain a competitive advantage.
- Personal data should *not be disclosed for a purpose other than for which it was collected*. A credit card company may not pass on its files to a car dealer, for instance.
- Personal data must be protected against non-authorized processing with appropriate organizational and technical security measures.

Registration

Switzerland has adopted a minimal database registration policy. In the private sector, the only data banks which have to be registered with the Data Protection Commissioner are those which:

1. record sensitive data or process personality profiles of people *on a regular basis*.
2. communicate stored personal data to third parties.

In both cases, however, the requirement to register becomes unnecessary if the data subject has been informed of the data files' existence. For example, if a company informs its employees in writing about its intention of compiling records on career planning for its staff, then it is not obliged to register the records.

In the public sector, all data files must generally be registered.

International Data Flows

The law is similar for the transfer of information abroad. Data file transfers from Switzerland must be declared to the Data Protection Commissioner if the communication is not a legal obligation or the data subject has not been informed. The details will be regulated by a *Federal Council Ordinance*. In certain cases, a simplified form of declaration can be put into operation - for instance, when an order involving personal data is passed on by a firm to a foreign subsidiary for further action.

Switzerland takes very seriously the principle of a free transborder flow of data. The government's view is that someone wishing to transfer data abroad should not be subjected to even stricter rules than they would encounter domestically if doing the same thing. The person transferring the data abroad would have to adhere only to the general principle that such a transfer must not in any way endanger the life or safety of the data subject. Such a situation could arise when the religious affiliation of an overseas employee is divulged

in a country that persecutes members of this religion.

The Right of Access

The new Swiss law also stipulates that everyone, i.e. each physical as well as legal person, can demand the right of access to his records from the data owner. An employee, for instance, may demand to see his personnel file.

But what happens when a firm wants to find out what information a rival firm has collected on it? This is not a simple question to answer. The law does give the data owner the right to refuse access to information if he can prove that his interest is superior to that of the data subject and if it does not communicate the data to other persons. This applies for instance when a firm demands access to its data only for the purpose of procuring information about the business practices of a rival firm. In general, however, the data that is provided should not constitute a violation of the data owner's rights.

A question often asked is who in a large company is responsible for communicating information? If a person wants to enquire about his particulars with a bank, for example, does he approach the head office or his branch office? There is no general answer to this question. Companies will have to adapt their data protection management in such a way as to be able to tell a data subject whom he can contact.

Data Protection in the Private Sector

Until now, we have covered the general provisions which apply broadly to both private data banks as well as to the federal authorities. We shall now turn our attention to data protection in the private sector.

Data protection is synonymous with the legal protection of privacy. Switzerland regulated the protection of privacy long ago in 1907 in its Civil Code. Article 28 of the Code stipulates that no one may violate an individual's right to privacy without adequate grounds. Should the case arise, however, the injured party may seek justice in a civil law court. He can demand the cessation of the violations and seek damages.

But when is an individual's privacy deemed to have been violated? The courts have never been able to solve this difficult question. Their standpoint is that constant observation by a neighbour constitutes a violation, or the spreading of false rumours which damage a person's reputation.

When, then, can *data processing* constitute an invasion of privacy? This is the question that the Swiss law attempts to answer, thereby plugging some of the holes in the Civil Code. The data protection law cannot regulate every imagineable situation. It can, however, set down certain principles and indicate in certain conflict situations the way in which data protection principles should operate.

The Swiss law seeks to answer two basic questions:

1. When does data collection and processing constitute an invasion of privacy?
2. Under what circumstances is such in invasion of privacy justifiable?

The answers provided by the new law are not final. An invasion of privacy is regarded as having taken place when the data protection principles described above have been disregarded. An invasion of privacy is also in evidence when data is processed against the express wishes of the person concerned. Such is also the case when particularly sensitive personal data or personality profiles are passed to third parties.

Balancing Private Sector Corporate and Data Subject's Interests

It is of course clear that these rules cannot always be adhered to on a day-to-day basis. There are times when the dominant interests of *a state, a third party or the data bank itself* will demand such a violation.

The bill therefore specifies that a violation of privacy is permissible if:

- it is specifically allowed by law;

- the data subject gives his consent;
- there is a dominant public interest, or
- a dominant private interest, for example, of the data bank.

One important question is how a data bank, i.e. a company, can make a valid claim to overriding interests? Swiss industry has always demanded that its special need for information be respected, and the Federal Council has largely acceded to this demand. The new law now gives hints as to when an industrial concern can make a claim of overriding interest. While they are not hard and fast rules, they do serve as pointers to how the law will be interpreted.

An overriding private interest can be evoked in the following instances:

- *When contracts are to be concluded.* Let us imagine a case where an airline has to find out the religion of a certain person and pass the information on to a security company so that the necessary precautions can be taken. Passing on this data in effect constitutes a breach of confidentiality since the person concerned did not consent to it. It is possible, however, that the airline is not always in a position to inform the data subject. Perhaps, too, the contract, i.e. the flight from A to B, can be fulfilled only if this information is divulged.
- *When assessing the creditworthiness of a firm, more facts may be collected than are absolutely necessary.* This violates the principle of proportionality, which constitutes an invasion of privacy. This concept means that one may collect only information, which is appropriate for the purpose for which it is intended to be used. But a company may be able to justify collecting more facts than is absolutely necessary to assess the creditworthiness of a firm. However, such over-collection may be unjustified when it is related to an individual.
- The *media* also enjoys certain privileges regarding personal data on a professional level. This means that the processing of personal data by the media is covered by the new law in so far as it relates to editorial material, but not, for example, in the organization's role as an employer where it enjoys no privileges.
- When data is processed only for *statistics, planning and research purposes* and published in a way that does not identify the data subjects.

Redress for Damages

Let us consider the example of a small carpenter's workshop which receives a very profitable order. The carpenter must obtain wood from the wood dealer. Before the wood dealer responds to the order, he makes inquiries with the credit company's information service about the carpenter's ability to pay for the wood. Because there is a mix-up, he receives the wrong information, to the obvious detriment of the carpenter. What course of action can the carpenter now take?

He can first of all demand that the false information is corrected. If he has not been able to execute his order and has incurred losses as a result, he has the right to claim *damages* against the credit company, and he can pursue his claim in a *civil law court* if it becomes necessary.

Management-Labour Relations

The law has a special provision for *management-labour relations.* An amendment to the standard labour contract will oblige employers to collect and process only as much data as is needed to establish a worker's ability to do the job or is necessary to implement his contract.

Enforcement

Responsibility for the management and enforcement of the new law will lie with the *Data Protection Commissioner* and a *Data Protection Commission,* as well as *the courts.* The Data Protection Commissioner will function as a kind of Ombudsman. He will have an independent status but be attached administratively to the Justice Ministry.

Although he will have no enforcement powers, he will be able to provide *recommendations* on data protection issues. He has the right to intervene in the private sector only if a company's data collection methods have adverse effects on a considerable number of people, or when data files must be registered, or data file transfers abroad must be declared. An example of the first case would be if an association of landlords were to keep a blacklist of tenants.

In less serious cases, however, the data subject has to deal directly with the data owner and pursue his claims in a *civil law court* if need be. Only a court has the power to impose fines and award damages against companies.

There are differences between the public and private sectors on the procedures in the event that the recommendations of the Data Protection Commissioner are not followed:

1. In the *private sector,* the Data Protection Commissioner may seek to have his recommendation confirmed by the Federal Data Protection Commission which can then hand down a decision. This decision may be challenged in the Federal Supreme Court.
2. In the *public sector,* the Data Protection Commissioner may seek to have his recommendation confirmed or not by the competent federal government ministry. A data subject may appeal against a decision of the ministry to the Federal Data Protection Commission. The decision of the Commission may be challenged in the Federal Supreme Court.

Privacy Laws & Business greatly appreciates the help given in the preparation of this report by Dr. Peter Muller and Mr. Jean-Philippe Walter, former and current heads of the Data Protection Service of Switzerland's Ministry of Justice