NEW-STYLE DATA PROTECTION LAWS: CONVERGENCE OR RADICAL CHANGE

Fifteen years separate 1973, when Sweden passed the world's first national data protection law covering the public and private sectors, and November 1988 when Australia passed its privacy legislation. Will the Swedish model of a comprehensive law, followed by most European countries in the 1970's and 1980's, converge with the self-regulatory privacy codes favoured in the USA, Canada, and Australia in a middle way; self-regulation within the law? Alternatively, do the second generation Finnish and Irish laws - soon to be followed by the Netherlands - represent a radical change?

In 1973, the main fear was that individuals' records were being held on mainframe computers, and that they had no way of finding out that these records existed. Not only was there no way to gain access, there was no way to ensure that individuals had a right of access. At that time, organizations considered that they owned the files, and gaining access was considered an infringement of the data owner's property rights. This is still the legal position in half the members of the EEC which have no data protection laws (Belgium, Greece, Italy, the Netherlands Portugal and Spain).

The Swedish model of a mass registration system was designed to give new rights to data subjects, and new rules for public and private sectors.

1. the existence of every data base in the country holding name-linked records would be centrally registered; (does a file exist?)

2. The Data Protection Authority has the power to give permission for file keepers to maintain certain sensitive files.

3. individuals are able to find out the types of data files each organization holds on them; (what sort of files are they?)

4. individuals can establish if the organization holds a file on themselves (have they got a file on me?)

5. individuals have a right of access to files on themselves; (I demand to see a copy of your record on me.)

6. data subjects have a right of correction, or at least a right to record their version of the facts if the parties cannot agree on the facts. (I demand to put the record straight).

This Swedish model was very influential in the way that legislation was drawn up and enacted in France, Denmark, Norway and Austria in 1978, Luxembourg in 1979, Israel and Iceland in 1981, the UK in 1984, the Isle of Man and Guernsey in 1986, and Jersey in 1987.

Germany - the odd man out?

Five years ago the German data protection law, passed in 1977, was seen as being the odd man out. One can now see with hindsight that it has many of the characteristics of what are now called second generation laws requiring a degree of self-regulation within the law.

The main principle in the German law is that the processing of personal data is permitted if the law allows it, or the individual has given his consent. This is different from the other countries which make the legal processing of name-linked data conditional on the file being registered with a central authority. In addition, in the German law:

* the data subject must be informed of the contents of a file when data on him is stored for the first time, unless he already knows about it;

* the data subject has a right of access to his data file for a minimal fee

* Incorrect data must be corrected;

* A data subject may erase data that is of doubtful accuracy, where the original need for its storage no longer applies, or where the data was not legally permitted;

* Personal data must be protected by adequate security measures.

Why should the German law should be regarded as self-regulatory? The reason is that the law requires any company carrying out a significant amount of processing of name-linked data to appoint a Company Data Protection Controller. The Controller must report to top management but be independent of it while carrying out his functions as Controller.

These principles have been worked into the new law in Finland, passed in February last year; the new law in Ireland, passed last July; the bill about to be passed in the Netherlands; and the Swiss bill which will soon begin to be considered in the Swiss parliament.

Why the Shift to the Self-Regulatory Model?

Why has there been such a shift in approach in the last few years? There have been three major factors: the rapid growth of microcomputers; the practical limits to enforceable regulation; and a reappraisal of data protection laws as alleged barriers to the free flow of data.

In short, the factors behind the shift towards second generation data protection laws can be best explained in terms of what is feasible in a democratic society. They have asked themselves: what is manageable, what is affordable, what should we concentrate on to achieve maximum results with limited resources?

Are the old-style laws converging with the new?

Will codes of practice and sectoral recommendations converge in the future with new-style debureaucratized data protection authorities? I think not. Self-regulation does not successfully work in the nuclear power industry, the stock markets, or any other area of life where there is inherent conflict between corporate and consumer interests. There may be common interests, for example, in the field of data security to counter hacking and computer viruses. Independent data security audits could play a

useful role in the absence of legislation, and could even check on a company's adherence to the OECD Guidelines on the Protection of Privacy. But the case for self-regulation alone remains unproven.

New-style data protection laws do represent a radical change from the old-style laws in that they offer a more meaningful role for corporate self-regulation. But by itself, self-regulation is not enough. There will always be a need for dissatisfied data subjects to appeal to an independent ombudman figure. While the traditional European approach may be seen as too legalistic and expensive, legislation is still needed to raise the awareness of data owners to their responsibilities to maintain high standards and comply with data protection principles.

In short, if the job of data protection is to be done, it requires legal requirements and legal sanctions. The challenge for companies is how, in practice, to manage self-regulation within the law.

Note: This is an edited version of the introductory address by Privecy Law & Business on the theme of our conference - Data Protection in Ireland, the Netherlands and Switzerland: Managing Self-Regulation Within the Law, held on October 19th in London. The papers are available from our office.