NORWAY PROPOSES PERSONAL DATA SECURITY REGULATIONS

All data protection laws contain clauses urging data owners and data controllers to adopt a data security policy appropriate to the sensitivity of each type of file. However, they generally give very little guidance on what organizations should do in practice. Denmark, Norway and Sweden are exceptions and have prepared regulations and guidelines.

In Norway, a working group was appointed by the Ministry of Justice in April 1986, chaired by the Data Inspectorate's Eirik Djonne. The working group drafted a proposal for regulations and completed its work in November 1987 (see PL&B August '87 p.5 and November '87 p.4). Since then, the Ministry has circulated the proposals for comment to about 40 organizations. It is currently taking a decision on whether the proposals should have the status of guidelines or regulations with legal force. As the proposals are lengthy, 26 pages in the recently prepared English version (available from Privacy Laws & Business), we will give only a brief summary.

The basis of the proposals is an evaluation of the files and parts of files into: not sensitive; less sensitive; sensitive; or highly sensitive. These degrees of sensitivity should be assessed in relation to the vulnerability of data subjects regarding, for example, their health, reputation, rights or financial position. The level of security depends on the file's sensitivity.

Under Norway's Personal Data Registers Act, the sensitivity of files covered by the general regulations, like personnel and payroll files, should be written into the regulations. For files requiring a licence, like credit information services and direct marketing agencies, the Data Inspectorate will decide on the degree of sensitivity of the files.

The 15 chapters of the proposals cover a wide scope, such as physical security, access control, network and communications security, and security for storage media and peripheral equipment. The first part of the document consists of a number of complex rules for evaluating security. The last part is simpler and covers the kind and level of security to be expected for different files in different data processing environments. These provisions cover: data quality; data collection, coding, registration and checking; interpretation of information; searching; data transmission; amendment and deletion; documentation of records; printouts; and checking results.

The Data Inspectorate has two major aims:

* to co-ordinate future development of data security for personal files with the development of wider computer security standards.

* to develop international harmonization for security requirements for equipment and services used for processing personal data files, in particular, common rules for security evaluation.

We propose a conference where the data security specialists from the Nordic countries meet company specialists to work out a practical common international approach to data security for personal data files. Please contact Privacy Laws & Business if you are interested.