

Technological Change

The Registrar follows developments, such as smart cards and document image processing. The latter technology uses optical discs. One twelve inch optical disc can hold the equivalent of 200,000 A4 pages of text. The DPR's office keeps up with such novel technologies to give guidance on how the data protection principles should be applied.

The Registrar's Future Activity

Over the coming years the DPR will concentrate on:

1. More contact with the different sectors to discuss their policies and promote good data protection policy and practice.
2. A more positive approach in monitoring compliance by enquiring into the practices of data users.
3. Continuing to handle effectively all complaints to his office.
4. Progressing with enforcement and prosecutions.
5. Further publicising his functions and the Data Protection Principles.
6. Reviewing the registration process.

This report by Andrew Winch, a county council strategic advisor, is based on a presentation by Francis Aldhouse, Deputy Registrar, at July's *Privacy Laws & Business 4th Annual Conference* in Cambridge. It has been edited and supplemented by the *Seventh Report of the Data Protection Registrar June 1991* published by HMSO, London, £11.40. ISBN 0 10 255391 2.

COMPLAINTS TO THE UK REGISTRAR SHOW NEED FOR TIGHTER MANAGEMENT

For the year ending May 31st 1991, the DPR received 2,419 complaints of which 31% related to consumer credit, up from 17% last year, and another 31% related to direct marketing. Over half (60%) of complaints are dealt with without the need for formal detailed investigation. On speed of investigation, just over one-third (36%) are dealt with within three months, two-thirds (67%) are dealt with within six months, and 9% take over a year.

Complaints to the UK's Data Protection Registrar show evidence of inadequate systems and staff training. These complaints have been selected from the DPR's Seventh Annual Report and provide an agenda for action for all to ensure that similar complaints could not be made against your organization.

Credit Reference

The complainant had encountered problems with her credit reference file. The financial dealings, including several debts, of a local company had been added to her file because they had wrongly been given her post code. The complainant wished to disassociate herself from the company involved. She also felt that this information had been the reason for her being turned down for credit. However, when she approached the credit reference agency they refused to remove the offending information.

The complainant was advised to have a notice of correction added to her file which would indicate that she was not financially responsible for the company in any way. This notice was added to the credit reference file although the County Court Judgements held against the company still showed her post code.

The credit reference agency was then warned that the way such data was held was in breach of the Fourth Data Protection Principle. This was because the personal data were inadequate and irrelevant for the purpose of

providing details of the complainant's credit worthiness. The credit reference agency agreed to remove the judgements in the name of the company from the complainant's file.

Direct Marketing

The complainant was concerned about receiving direct mail from an organisation. Attempts were made to get this stopped, but he continued to receive mailings.

Formal action was considered necessary to remedy the situation and the Registrar served an enforcement notice for contravention of the First and Fourth Data Protection Principles. The First Principle was breached because the company had unfairly processed personal data relating to the complainant resulting in the despatch to him of unsolicited promotional literature despite his request to the contrary. Also, the Fourth Principle was breached because the data user held personal data which were inadequate in relation to the purpose for which they were held. This was because they were not marked so as to ensure that such literature would not be despatched against the complainant's wishes. The data user did not appeal against the notice.

However, despite this, a further mailing was sent to the complainant. The data user was then prosecuted for failing to comply with the enforcement notice. The data user pleaded guilty and was fined as well as being ordered to pay prosecution costs.

Data Security

The complainant purchased a washing machine from a high street store and was asked to complete an application form for credit. Details from his application form were entered into a computer and he was horrified to find the personal details, which he provided on the application form, were displayed on a VDU positioned about 6ft high on a shelf and clearly visible to other customers in the store. He complained to the store manager and subsequently to the Registrar.

A regional investigator visited the complainant and the store. Although the

position of the VDU in that particular store had been changed, it appeared that there was a problem in other stores. It also appeared that staff generally were not aware of their obligations under the Data Protection Act.

The company reviewed the location of all VDU's in its stores and found that there were a number where information could be read off the screen by the public at large. The company was in the process of replacing computer equipment and assurances were given that the position of the new VDU's will ensure compliance with the security requirements of the Eighth Data Protection Principle. The company sent gift vouchers to the complainant in recognition of the embarrassment caused to him.

Processing Personal Data Outside The Terms of Registration

The complainant was receiving unsolicited mail as a result of enquiring about the products of a mail order company. Upon investigation it became apparent that the company to whom the complainant had originally enquired, had sold its customer list to another similar company. The customer list was subsequently made available to other companies on behalf of the new list owner, by a list broker.

The company that had purchased the list was, at that time, only registered under the Data Protection Act as a Computer Bureau. The Registrar prosecuted the company for holding personal data while not being registered; the company pleaded guilty and was fined.

Subject Access and Staff Training

The complainant had made a subject access request to a local authority without getting a reply. Following investigation, the authority explained that the problem was due to an administrative error and apologised to the complainant. Assurances were given to the Registrar that the relevant personnel are now properly aware of the subject access provisions of the Act.