UK REGISTRAR TARGETS WIDE RANGE OF ISSUES IN HIS TENTH ANNUAL REPORT

In his final report, published in July, the UK's retiring Data Protection Registrar, Eric Howe, targeted a wide range of issues.

The EU Directive's Jurisdiction Problems

Article 4 of the Directive requires Member States to apply the directive to *controllers* of data established within their jurisdiction. The law of the member country where the parent organisation is based will apply. For instance, an Italian company collecting and processing data on British citizens in the UK would be subject to Italian law through its parent company in Italy.

The Registrar thinks that this approach does not give proper protection to individuals. He is not convinced that it is right for a UK citizen to seek redress in Italy if the data is collected and processed in the UK. This also applies in the reverse case; where an Italian citizen would have to seek redress in the UK if the terms of the Directive are breached. Indeed, the Registrar's points out that it would be difficult to ensure that decisions taken in the UK would be implemented in another country.

Mr. Howe expresses concern that other directives raise data protection issues; such as ones that deal with communication, banking, insurance and distance selling. He fears that the EU might end up with a mixture of differing data protection regulations. He understands that if a clash arises between the data protection directive and other directives, the data protection legislation should prevail.

He also gives details of developments affecting police forces, customs and drug control units across the EU and calls for more collaboration between the Data Protection Commissioners and the establishment of working parties dealing with several European developments on the data protection front.

Pressure for National Identity Numbers

Since last year, there have been a significant number of parliamentary questions to Ministers about policy on a national identification system. Mr. Howe is concerned about a number of current and proposed public identification systems such as driving licences bearing the holder's photograph, social security swipe cards, national insurance and national health service numbers. The new money laundering regulations require financial institutions to insist on proof of identity of customers, which will add to pressure for a common identification system.

Two nationally allocated numbers already exist - the National Insurance number and the National Health Service number. In some cases, the National Insurance number is already being used as the income tax reference number and in matching insurance files. If pressure continues for a national identification system, then a full and informed debate on the nature of such a system should be carried out as a careful evaluation of the pros and cons will be needed.

Confidentiality vs. Disclosure

Confidentiality and lawfulness in relation to the processing of personal data was considered in a consultation paper in January 1994 (PL&B September 1994, p.16). It sought to solicit a response to the Registrar's view of the way in which a duty of confidence affects the processing of personal data in the finance industry. It is his view that some of the finance industry's current and proposed practices could entail the unlawful processing of personal data. Organizations in the finance sector disclose to each other confidential information on their customers' accounts, generally, through credit reference agencies. He acknowledges that disclosure is necessary in some circumstances. However, the duty of confidence may still apply in these cases. In his opinion, express consent of the customer is needed for disclosure of personal data held under a duty of confidence.

Guidance on Health Data Urgent

There is a need for additional safeguards regarding health information which is covered by the law of confidentiality. As information has to be obtained and processed lawfully, *implied* consent is not enough for the National Health Service (NHS) to use data for a purpose different from the one for which it was originally collected.

The Department of Health has been promising guidance on the confidentiality of health information for a number of years. Consultation between the Registrar and the Department of Health have centred on the extent to which patients should be given an opportunity to "opt-out" of any uses and disclosures which are outside the scope of their treatment, particularly if the information provided should be used for research.

Several other data protection issues within the NHS are examined in this year's annual report. These include:

- ethnic monitoring
- the mentally ill
- genetic screening.

Action Needed on Personal Data Market

In last year's annual report, the Registrar expressed concern about the existence of a market in personal data by which third parties could gain unauthorised access to individuals' bank accounts. The Data Protection Act did not seem to provide effective protection for such cases.

After gaining some publicity from a newspaper investigation in late 1992, the matter was brought to public attention again, early in 1994, as a result of an advertising campaign by an investigation agency. Letters were sent by the agency to Members of Parliament and Members of the House of Lords offering to supply details, such as personal calls, mortgage repayments, bank balances, for a fee. As a consequence, in March this year, the Minister of State at the Home Office, Earl Ferrers, stated that there was a need to make it clear "beyond doubt that a person who obtains unauthorised access by deception to personal data is guilty of an offence. We shall be seeking the necessary legislative provision to make amendments to the law in that particular case."

The Registrar welcomes this view. However, it seems that it is not enough to deal with this issue under the Data Protection Act. A change in the Criminal Law might be needed to cover this type of offence.

DPR and Police Review Criminal Records

The Registrar expresses concern over PHOENIX, the forthcoming National Criminal Records System on the Police National Computer. Discussions between the Registrar and the Association of Chief Police Officers (ACPO) included the following issues.

1. Retention Periods for Criminal Records. The establishment of the new system re-opened the issue of how long criminal records should be retained and the circumstances in which they should be deleted. Although ACPO modified some of its original proposals for extending the periods for which criminal records should be retained, the PHOENIX system itself presents a problem in that the system is not restricted to conviction records alone - it also contains the names of persons acquitted of crimes. In two cases, the Sexual Offences Act 1956 (section 6(3)) and the Theft Act 1968 (section 27(3)), it may be necessary to retain acquittal records for a period of time in relation to offences where certain defences can be used only once.

A further issue is the conversion of the National Identification Bureau's existing manual records into a form suitable for computer processing. This operation might take place outside the UK. But the Data Protection Act would still apply, as the data would be controlled from and used within the UK.

2. Disclosures of Criminal Records. The Home Office issued a consultation paper on the disclosure of criminal records for employment vetting purposes.

Concerns are expressed by the Registrar that such disclosures raise some difficult questions of public policy. There should be a careful determination of who should have access to criminal records and in which circumstances. Arrangements should also be made to protect the individual about whom requests are made.

3. DNA Databases. There have been proposals to create large scale DNA profile databases in the past, although none have been established until now. Nevertheless, issues remain relating to data derived from samples taken in the course of routine criminal investigations.

4. HIV/AIDS Markers on the Police National Computer (PNC). In last year's annual report, Mr. Howe reported that a Home Office circular had recommended the removal of markers on the PNC which indicated an individual's HIV status. The circular concluded that the best protection for police officers was the adoption of standard hygiene procedures whenever circumstances might bring them in contact with blood and body fluids. By adopting these procedures there would be no need for the existence of markers. Such procedures should have been completed by the end of 1993, when the markers should have been removed.

It seems that the process of issuing the central guidance on training was delayed. However, the Registrar's staff have contacted all Chief Police Officers to check the progress towards the deletion of the markers. It seems that only a few continue to retain such markers. This retention may contravene the fourth Data Protection Principle.

Open Government Includes Manual Data

In July 1993, the White Paper on Open Government was published; it set out a code for access to information held by central government. One of the proposed statutory rights would give individuals the right of access, subject to exemptions, to manual records held by the government about them. This approach is welcomed by the Registrar as it extends existing rights of subject access to computer records under the Data Protection Act to an extensive class of manual records.

Many Child Support Agency Complaints

From late 1993, the Registrar's office has received a great number of complaints about the CSA. The majority concerned the disclosure of income information in maintenance assessment notifications. Other complaints related to disclosures of information by employers, mis-identification of individuals and whether some CSA literature is misleading in its references to confidentiality. Many complainants believed that information could not be disclosed without permission of the relevant individual under the Data Protection Act - this view is incorrect. Nevertheless, a close examination of the situation suggested that the CSA was disclosing more information than expressly required to do by the regulations made under the Child Support Act 1991.

The regulations require the assessable income of an absent parent to be disclosed to the parent with care, and vice versa. The calculations take into account the incomes of others in the absent parent's current household. In some cases an indication of the income of the absent parent's new partner was disclosed.

Maintenance assessment notifications must include protected income "where relevant." (Protected income is a minimum disposable income for absent parents which they should not fall below as a result of paying maintenance to their children). Therefore, the Registrar suggested to the CSA that the protected income level should only be disclosed in cases where it actually resulted in a reduction of the maintenance payable by the absent parent. The CSA has now restricted the amount of such information disclosed at the request of the Registrar.

Disclosure and Use of Banking Data

The "Good Banking" Code of Practice
A review of the Code was published in May 1994. Paragraph 10.1, dealing with the marketing of their services, states that: "Banks and building societies will not make the

provision of basic banking services conditional on customers giving such written consent (to the disclosure of names and addresses to other companies in the same group for marketing)."

This change from the previous year's version is welcomed by the Registrar. However, the duty of confidentiality also restricts the *use* of data and not only the *disclosure*. Thus, it is the Registrar's view that customer information cannot lawfully be either *disclosed* or *used* for marketing purposes by third parties, including companies in the same group, without the consent of the customer.

The Security of Banking Information

This issue is closely related to the existence of a market in personal data. Twelve banks were visited by the Registrar's staff to discuss the security of customer information. The meetings provided an overview of the variety of security measures in place and demonstrated that significant steps had been taken by the banks to strengthen their systems and procedures in order to avoid unauthorised access to customer information.

However, complaints were received by the Registrar about disclosure of customer data over the telephone which raises particular security problems.

Insurance Industry Launches Data Code

It is well known that insurance companies handle a great deal of sensitive personal information about their customers. In December 1993, the Association of British Insurers (ABI) published its Data Protection Code of Practice (available from the PL&B office or the ABI, 51, Gresham Street, London, EC2V 7HQ. Telephone: 071 600 3333 Fax: 071 696 8999) which gives useful advice to those in the insurance industry.

Other developments in the insurance industry include the creation of industry-wide databases:

- **CLUE (the Comprehensive Loss Underwriting Exchange)** is a database system through which insurance companies will share insurance claim data. It will also be used for fraud prevention and underwriting purposes.
- **The Impaired Lives Register** is a centralised insurance register containing details of individuals who have been refused life insurance cover or who have been supplied with life insurance cover at an increased premium due to health reasons. The Data Protection Act applies to the register as the information held includes a shortened version of the name of an individual, date of birth, insurance company and the category of the insurance policy. With regard to supplying information to the register, insurance companies are using personal data for a purpose different from life insurance administration; applicants should be made aware of this fact. The ABI has included a clause in its code of practice asking insurance companies to draw attention to the register in life and permanent health proposals and application forms.

Enforced Subject Access to be Banned?

The Registrar believes that the practice of requiring individuals to exercise their rights of subject access to criminal records and national insurance records by some employers in their employee selection procedures should be prohibited. He has expressed his concerns about enforced subject access many times before, and continues to stress that it is a clear abuse of individuals' rights. Nevertheless, the practice continues to increase.

The National Identification Bureau reveals that 11,500 subject access requests were made for information from the Police National Computer system in the year to March 1994 (see page 26). The Department of Social Security has also reported over 12,500 requests over a similar period. Both authorities believe that over 90% of the requests result from enforced subject access.

Practices, Technologies and Techniques

Many of the new developments in computing and communications technology

may have significant implications for data protection. Major developments include: Calling Line Identification, the Internet, and Document Image Processing (PL&B September '94 p.19).

1. Calling Line Identification (CLI). Calling Line Identification issues have featured in the Registrar's eighth and ninth reports. His view is that CLI services should give the person making a telephone call the opportunity, at no charge, to suppress the transmission of his/her telephone number. The suppression should be possible on a "per call" basis - *call blocking*, or by blocking all transmissions from a particular number - *line blocking*. It seems that both UK telecommunication carriers, BT and Mercury, will make the suppression available at no charge.

2. The Internet. On the Internet, users of various networks around the world are able to communicate with eachother without any restrictions. They communicate freely using electronic mail and bulletin boards, transferring files and accessing a wide range of readily available information.

Several reports suggest that the number of Internet users now exceeds twenty million, and the figure is growing fast among both the commercial and academic communities.

The Internet presents many data protection challenges. The use of the network for transferring personal data is subject to the same legal constraints as the use of a private network or, indeed, any other means of data transfer. Responsibility for meeting data protection requirements, such as accuracy and security rests with the transmitting data user. However, there are other issues of concern. How can transborder data flows be regulated? How can privacy safeguards be established and enforced? It remains to be seen how the new Registrar will approach these issues in future.

Lawful Use of Customer Information by Utility Companies?

Regional Electricity Companies (REC's) use and disclose information for a number of purposes. The question is whether such activities are lawful. The issues apply to other utility companies as well. They are in a unique position as they have a comprehensive customer list with a very high response from customers who notify them of name and address changes.

The Electricity Act 1989 restricts the use and disclosure of customer information by REC's. The *ultra vires* rule may also restrict the powers of the REC's. It states that organizations which have statutory powers are only able to do that which Parliament has allowed them to do. In the case of electricity companies, the Electricity Act restricts their contractual freedom to deal with customers.

It is the Registrar's view that a number of current and proposed uses and disclosures of information by the REC's, contravene the Electricity Act restrictions. Formal guidance will be issued later this year.

Complaints to the Registrar Down

The Registrar's Office has received 2,889 complaints this year - considerably fewer than the 4,590 of the previous year. (The previous year was exceptional due to a TV advertising campaign run in March 1993, after which there was an average of 56 complaints per week compared to 33 per week before the campaign). However, there has been an increase over the 1991/92 year.

Over three-quarters (78%) of all complaints were about data users in the private sector, the majority within the finance industry. Complaints related to consumer credit (about the accuracy of the information held by credit reference agencies) accounts for 31% of all those received, down from 63% last year.

Other issues in the Data Protection Registrar's 10th Report include: new databases on those who have changed address and defaulted on loans, geographic information systems, data matching, and smart cards.

Tenth Report of the Data Protection Registrar, HMSO HC453. Price £12.25

This report was written by Dr. Deborah Fisch Nigri, a *Privacy Laws & Business* consultant.