U K ready for November 11?

The UK government ratified the Council of Europe Convention (for the Protection of Individuals with regard to Automatic Processing of Personal Data) on August 26th this year (see page 1). The Data Protection Registrar's office is now up to date with adding new applications from data users and computer bureaux to the Data Protection register. A copy of the register is available for public inspection in over 170 main public libraries, one in every UK local authority area. The stage is set but what will happen when the drama begins? On November 11th, individuals will gain a right of access to records on themselves (at a maximum fee of £10 per register entry) and Eric Howe, the Data Protection Registrar, gains his full powers to enforce the law. PL&B visited the Registrar's office at Wilmslow, near Manchester and spoke with Eric Howe and his departmental heads to find out how they are preparing.

The Registrar's Objectives

Eric Howe's four main objectives are to:

1. Strengthen the rights given to individuals and resolve their data protection problems by providing an effective Ombudsman service.

2. Promote the good practice contained in the Data Protection Act's Principles by encouraging and supporting the development and adoption of appropriate codes of practice, procedures and techniques by data users and their representative organizations,

3. Establish openness in the use of personal data by maintaining and publishing a register of data users and computer bureaux as required by the Act.

4. Seek to ensure that the Act is properly enforced at minimum complexity and cost both to data subjects and data users.

1. STRENGTHEN INDIVIDUAL DATA SUBJECT'S RIGHTS

Although the Registrar does not have his full enforcement powers until November 11th, he nevertheless received 225 complaints in the year from July 1986 to June 1987 and his public office gives him considerable powers of persuasion to resolve problems. Around half of the complaints are resolved by correspondence and the other half require a deeper investigation. The aim is a mediated solution, an approach which will be continued even after November 11th. However, the Registrar will make an enforcement notice, if necessary. He will also take up a problem with a trade association or other representative body if an issue affects a whole sector. Ultimately, the Registrar may prosecute a data user who refuses to comply with an enforcement notice or flouts the law in some other way, for example, by refusing to register when he should do so.

Indeed, since September 12th 1984, individuals have had the right to initiate private prosecutions to seek compensation through the courts for any damage and associated distress suffered on or after this date arising from:

* the loss of personal data relating to him, or

* a person gaining access to the data or its destruction or disclosure without the authority of the data user or computer bureau.

In addition, from May 11th 1986, individuals have had the right to gain compensation through the courts for damage and associated distress suffered on or after this date because of inaccuracy of personal data. The court may also order correction or deletion of inaccurate personal data. However, as far as the Registrar is aware, there have not yet been any such private prosecutions.

John Lamidey, Head of Investigations, explained how his department deals with complaints. The Investigation Department deals with all complaints but undertakes an investigation only where there are complaints of substance in terms of the Act, for example, that a company is using data for a purpose other than one which is registered. Sometimes, what appears to be a complaint is really a person seeking advice. So the first question to be asked is whether a "complaint" really needs investigation. For example, if a person writes to the Registrar to say that his company is not registered when in fact it is, a simple reply letter quickly resolves the "complaint." Most people writing in, simply require information. If necessary, the individual is re-directed to the appropriate body, like the Advertising Standards Association.

In addition to the complaints which can be resolved by letter, the Registrar's office also receives complaints of substance like those suggesting that a company is not adhering to the Data Protection Act's Principles. To deal with this type of complaint, Lamidey has recruited a team of investigators, and one will be based in each of the 12 regions into which the UK has been divided for this purpose. He has deliberately chosen investigators from a wide range of backgrounds so that he can offer a flexible response to any situation which is likely to occur. For example, an ex-policeman may be more suitable for some situations (like dealing with a refusal to register), while an ex-personnel manager or social worker may be more appropriate in others (like helping complainants having difficulty exercising their right of access, erasure or correction to records on themselves). Regardless of background, all receive a common training. At this stage, the full-time investigation staff are few and the others are employed on a part-time basis as necessary.

What do people complain about?.....

So far, most complaints have been about the private sector:

* some 30% of all complaints have been from people who had received unsolicited mail and who would like to stop it (see page 13 for a report on the Direct Marketing Code of Practice and the Mailing Preference Service).

* The next most important area has been complaints about financial activities, like the provision of credit reference information. The main problem here is its relevance. For example, sometimes a credit reference (information) agency gives a credit provider information not only about the individual seeking credit but also about other current or past occupants of his house. The Registrar is currently discussing this and related issues, like the establishment of a National Credit Reference

Register, with the Finance Houses Association, the British Bankers' Association, the Building Societies' Association and leading companies like Infolink.

* Around 11% of complaints have concerned the use or disclosure of information in a manner incompatible with the purpose for which it is held.

* A further 12% of complaints have been about possibly inaccurate data.

Here are some examples covering both the Act's principles and its definition of data.

1. Fair and lawful collection (1st Principle), data to be held only for the lawful purposes described in the register entry (2nd principle), and data must be adequate, relevant and not excessive in relation to the purpose for which it is held (4th Principle)

The complainant received a questionnaire from his bank. The covering letter with the questionnaire stated that the bank was ensuring its data was accurate to comply with the Data Protection Act. As the questionnaire asked for some details which the bank had not requested previously, the customer saw this as using the Act to increase the quantity of personal data held by the bank.

The bank later explained to the Registrar that the questionnaire was, in fact, for two purposes:

(a) to ensure that the data was accurate to comply fully with the Act;

(b) to hold enough data to offer its customers a wide range of banking services.

As a result of the Registrar's intervention, the bank agreed to re-draft its covering letter to make it clear that there was a marketing purpose to the questionnaire. The complainant was assured that he was not obliged to complete the questionnaire.

2. Use/Disclosure compatible with registered purpose (3rd Principle)

A bank customer received unsolicited mortgage repayment quotations from three insurance companies. The quotations contained the customer's name, address, date of birth and current mortgage repayment details. The customer considered that these details should be confidential to his bank and should not be disclosed to a third party.

After the Registrar intervened on behalf of the customer, the bank promised not to pass identifying details in this way in future, even though the bank is registered under the Act to disclose information to other firms for marketing purposes.

3. Act's definition of data as automatically processed information and the overseas transfer of data

The complainant received an envelope, posted from Amsterdam, the outside of which identified the complainant, with her full address, as a credit

card holder. The complainant objected to the details being transferred abroad and the details being printed on the outside of the envelope.

The company stated that the data was transferred abroad in the form of address labels. Therefore, and the Registrar agreed, there had not been a transfer of data abroad under the terms of the Data Protection Act. However, the company agreed that in future it would not identify individuals as credit card holders on the outside of its envelopes.

In the first example, the complainant was shown to be fully justified and in the second example, the complainant was shown to be right in the spirit but not the letter of the law. However, in the third example, the company was shown to be operating completely within the law regarding overseas transfers but not regarding protecting the privacy of an individual, identifying her as a credit card holder.

2. PROMOTE GOOD DATA PROTECTION PRACTICE

The purpose of codes of practice is to relate the Data Protection Act's provisions to the everyday practice of specific sectors. The first two codes of practice to be published were those of the Association of British Travel Agents (ABTA) in March 1987 and of the Advertising Association, in April 1987.(see page 15). The Advertising Association (AA) provided a valuable coordinating function for a working party consisting of the Institute of Practitioners in Advertising, the Association of Market Survey Organizations, Freemans (a major mail order company), the Direct Mail Producers' Association, the British Direct Marketing Association, the Association of Mail Order Publishers, the Post Office, the Incorporated Society of British Advertisers, the British List Brokers' Association and the AA itself. The above trade associations most closely related to direct marketing have committed themselves to observe the code both in letter and in spirit and have made such a commitment a condition of their respective associations.

Both ABTA and the AA approached the Registrar to seek his help in drawing up their codes of practice, which took over a year to complete. Even so, both the Registrar and the trade associations recognize that this work may be revised in the light of experience.

The Registrar, in welcoming the AA code of practice, clarified its status as a voluntary code within the law. He states, in the foreword, "Observance of this Code does not constitute an assurance that I will accept in all cases and without qualification that data users have complied with the Act. However, in considering relevant complaints it is my intention to give careful regard to whether the data user concerned has been complying with this Code of Practice and will take such compliance as a positive factor in his favour."

Other sectoral codes of practice are being prepared by the Association of Chief Police Officers, the Universities, the British Computer Society, the Institute of Administrative Accountants, and the Local Authorities. In addition, a number of guidelines are being prepared to cover issues that apply regardless of industry, like personnel records and data security, by the National Computing Centre, the Institute of Personnel Management and the Institute of Chartered Accountants.

3. ESTABLISH OPENNESS WITH THE REGISTER OF DATA USERS AND COMPUTER BUREAUX

The Data Protection Register is the Registrar's largest administrative task, employing 12 people (down from a peak of around 50), and the importance of the task gives Eric Howe his official title of Registrar. However, it is not number one in his list of priorities because he does not regard the Register as an end in itself. It is rather a means to give transparency to the processing of name-linked data. The public register has two functions. The register provides:

1. a full description of an organization's use of personal data

2. individuals with an address to establish whether an organization is using data on them and, if so, obtain a copy of that information.

This will enable them to exercise their data subject access rights and check whether an organization's data on them is being used in accordance with the data protection principles, like accuracy, relevance and other attributes of good data protection practice. In short, companies should not consider that they have complied with the law merely because their registration has been accepted. On the contrary, it is just the start because they must comply with the data protection Principles in their everyday operations. Furthermore, the organization must process data within the terms of their register entry and must keep their register entry up to date.

Mike Duffy, Registration Manager, explained how the registration system works. First, the statistics. By the end of August 1987, there were 131,000 entries on the register, representing 110,000 organizations, an average of 1.2 registrations each. The most commonly used purposes are:

+ Personnel/Empoloyee Administration (including payroll), registered by 49.1% of data users

+ Customer/Client Administration (including sales ledger), registered by 35% of data users

+ Purchase/Supplier Administration (including purchase ledger), registered by 33.9% of data users

+ Marketing and Selling (including direct mail), registered by 20.5% of data users.

Although all automated name-linked data files should have been registered by May 11th 1987, registrations are still being sent into the Registrar's office at a rate of around 1,000 a month. In addition, data users are sending in amendments to register entries at a rate of around 1,500 a month. The latter are entered onto the register in on-line mode.

Mike Duffy explained the registration procedure. There are three stages:

+ The clerical check is to ensure that a registration application is complete. This means, for example, that the fee of £22 (going up to £40 from November 11th 1987) has been enclosed, and that the declaration (that the

information given on the application form is correct) has been signed by the person representing the data user. The clerical staff send all applicants that pass this check an acknowledgement, but about one in ten fail at this stage and they are sent a note seeking the extra information or missing registration fee. The cheques are paid into the bank and then the application forms are sent for inputting into the computerized Register.

+ The validation of the applications consists of a series of simple checks to ensure that the applicant's description of his use of personal data (in terms of data subjects, data use, source, disclosure, and overseas transfer) is comprehensive and clear.

+ Once the application has passed these checks, which may involve a discussion with the applicant, it is entered onto the Register.

The Registrar has commissioned research from which it is clear that there are thousands of particularly small business data users who have not yet registered. To ease their task, the Registrar has piloted a simplified registration form which covers the four most popular purposes, as indicated at the beginning of this section. The simplified form will be available from September 1987.

4. ENSURE THAT THE ACT IS PROPERLY ENFORCED

Apart from handling complaints, described in the first section, the Investigations Department also identifies those data users which have failed to register. Although it has been an offence since May 11th 1986 to be a data user without being registered, no-one has yet been prosecuted. However, the first prosecutions are expected in the next few months.

The investigation technique is to check against the registrations published lists (like trade associations) of organizations that are likely to be heavy users of name-linked data. The first checks were made in December 1986 and even-handedly covered both the public sector, (local authorities and health authorities), and the private sector, (direct mail and mail order companies).

When companies are found to have not registered, they are sent a letter asking if they process name-linked data. They are asked to reply within two weeks. Then, according to circumstances:

* the organization will become registered, or
* they have no need to register, or
* they may refuse to discuss the situation with the Investigation Department.

Organizations that do not reply to two letters from the Registrar's office will receive a surprise visit, which ultimately could lead to a prosecution. John Lamidey, Head of Investigations, assures PL&B readers that no-one will be prosecuted without these preliminary efforts to encourage compliance with the law.