HOW ICI RUNS ITS UK DATA PROTECTION ACT COMPLIANCE PROGRAMME

We examine how one major UK company, ICI, has approached the issue of complying with the Data Protection Act, how it has used the legislation to maintain and improve the awareness of its managers and staff, and how it is approaching the - for some - vexed issue of subject access.

To be certain of remaining within the law the company set out to ensure that those who control collections of data within the enterprise and those who have primary and secondary access understand their obligations under the Act in general, and in respect of subject access and disclosure in particular.

Data Protection Corporate Policy Group Established

Early on, therefore, a small group was established at a corporate level to organise compliance with the Act. It comprised a triumvirate of senior members of the personnel, corporate management services and company secretary's departments. One of its first jobs - as in many other companies - was to initiate and oversee ICI's registration under the Act.

In the case of ICI, to ensure that the completed registration form accurately recorded the whole spectrum of its storage and use of personal information, a method was devised actively to involve those in the company with knowledge of the information required by the UK's Data Protection Registration form DPR1 form. Because of the diversity of ICI's use of personal information and the composite nature of the company more than one form was necessary. A step-by-step approach was therefore adopted. A first draft of the set of the company's DPR1s was drawn up and circulated as widely as possible through ICI divisions for correction and comments. These were incorporated and a second draft circulated; this process was repeated until the DPR1s accuratedly reflected ICI's use of information covered by the Act, and the structure of the company. It was also at this stage that thought was given to the Act's future requirements on subject access in producing a set of forms which had an appropriate internal structure. The result of the registration exercise for ICI was a multiple registration with 14 part A forms and 20 part B forms.

In tandem with the circulation of the draft set of registration forms, an information card was also circulated to raise awareness amongst all potential users of personal data. It sets out in a convenient form ICI policy and the basics of the legislation.

Part-time Data Protection Coordinators Appointed

In addition to the above, a "network" of data protection coordinators was established. Professional staff with the appropriate knowledge and experience of information processing in a wide range of jobs were designated as coordinators. At ICI, in contrast with some other companies, full-time data protection officers, as such, were not appointed. ICI saw this approach as having a number of advantages, in particular:

* it avoided a separate and costly data protection bureaucracy;

* because coordinators remained in their existing positions they did not become distant from the practical day-to-day issues of information handling;

* coordinators hold diverse positions within the company (for example, personnel officers, computer systems staff, administrators). This means that the "network" is formed of a multidisciplinary team;

* department heads rather than full-time data protection officers remain fully responsible for the correct use of personal data by their staff and for ensuring that the company does not break the law.

The coordinators were briefed by the central working group at a series of meetings. In the early stages these meetings were held relatively often, but in the future it is not envisaged that such meetings will be required more than twice a year. Because the coordinators are a multidisciplinary team and remain in their existing jobs, the company finds there is a valuable exchange of views and information at these meetings.

Raising Employee Awareness

Armed with the information card, a management guide to data protection and a company policy statement on disclosure, the co-ordinators talked to managers, arranged seminars and generally raised awareness of company policy and the Data Protection Act amongst managers and staff.

In addition, data protection awareness is being maintained through ICI divisions' staff handbooks. A model paragraph has been made available to those responsible for updating the handbooks in different divisions of the company.

Amending ICI's registration forms

ICI sees the question of data protection very much as a continuing process. The data protection coordinator network and the central working group continue to monitor developments and initiate changes. For example, since initial registration, amendment forms - DPR2s - have been submitted to the Registrar, updating the company's entries. When new legal entities within the ICI group are created, registration and compliance with the Data Protection Act are kept in mind as a matter of course. This process is helped by having someone from the company secretary's office as a member of the data protection working group.

Disclosure of Data

Disclosure of personnel data both within the company and to outsiders has always been tightly controlled at ICI. Following the DPA, however, the company took the opportunity to draw up a statement of policy and a management guide, restating its existing practice. In developing its own management guide, ICI made use of the disclosure categories in the registration document.

Under the DPA, disclosure is only authorised if both the purpose of the disclosure is compatible with the listed purpose and the person to whom the information is disclosed is listed on the data user's registration entry (Part B) or else is covered by one of the "non-disclosure exemptions." The exemptions include disclosures made with the data subject's consent or required by law. The registration provisions of the Act give companies a wide range of policy options on the registration of disclosures. They may:
1. register all disclosures and deal with non-registered requests for disclosure by obtaining specific authorisation from the employee concerned.
2. register no disclosure whatsoever and rely on the statutory exceptions to disclose without the employee's consent where this is required by law or to seek the employee's consent.
3. register certain less sensitive disclosures and seek the data subject's consent for all other disclosures.

Companies may opt for restricted disclosure as in 3 in order to create a climate of greater trust in which employees can be confident that the privacy of confidential information supplied to the employer will not be breached without their permission.

ICI strongly favoured restricting disclosure entries in the registration entry and extensive recourse to data subjects for explicit consent. The company took the view that, because a registered disclosure does not require data subject consent and does not provide any opportunity to reassure data subjects as to the circumstances in which a third party disclosure would occur, it would deliberately minimise its registered disclosures. In doing so, the company relies heavily on the exemption provided when the data subject's consent is given and on the other statutory exemptions. Instead ICI has produced its own internal code of practice with examples of the circumstances in which it would disclose and the conditions which must be met prior to disclosure. This management guide is both a set of instructions and a basis for reassurance to its employees. The company believes that this reflects its concern to give pride of place to the quality of its relationships with employees as data subjects.

Data Subject Access Policy

ICI does not expect a great many subject access requests and expects more from employees than from other data subjects (eg.customers)

Its existing and pre-Data Protection Act practice has been to provide access to the employee record documents (computer produced in most cases) and to the employee's personal dossier, on request. In practice the company has had few such enquiries and on grounds of accuracy it regularly uses a campaign approach in taking initiatives to get employees to check and update their record.

ICI believes that most of the requests will be capable of being discussed face to face, doubts whether the requester will be familiar with the terms of ICI's registration entry and does not expect the employee to refer to it. It envisages such a discussion identifying the areas of interest and concern and enabling researches to be defined and initiated. Personnel officers will be equipped with knowledge of the main collections of data, some at least of which will contain personal data concerning the requester. The basic employee

record can be printed out on-line within five minutes of a request being made in most of the company's personnel offices.

For normal requests from employees, ICI expects to waive its right to extract a fee. If it is felt appropriate, an access application form will be used. This is most likely where the company is in correspondence with a recruitment candidate or a former employee or where it is progressing multiple searches. An "all you have on me " request might need to be extended to other geographical locations. However, such is the potential complexity and cost of searching in response to an "all you have on me" request that ICI has reserved the right to charge in certain circumstances.

ICI's approach in summary

There are a number of key aspects of the company's experience which may be of general interest and relevance.

Bureaucracy - The company managed to avoid the establishment and growth of a data protection bureaucracy by deploying existing human resources in a coordinating "network".

Involvement of experience - The network of data protection coordinators form a multidisciplinary team drawn from staff with direct involvement and experience of handling computerised personnel data, and these people remained in their ordinary jobs.

Responsibility - Departmental heads are responsible for ensuring that the company's policy on personal data is adhered to and that the company complies with the Act at all times. There are no separate data protection officers, as such, given or assuming this role.

Awareness and publicity - The company used the Act, and the data protection principles in particular, as a touchstone to test its developing policy and practice. Appropriate publicity materials for managers and administrative staff were developed and deployed at all levels throughout the company.

Monitoring and planning - The company keeps abreast of legislative developments and interpretations of the Act and thinks through the possible implications for its policy and practice (eg.subject access provisions).

Trade Unions - At an early stage, two of the trade unions represented at ICI approached the company requesting information on the steps ICI was taking in respect of the Act. The company replied to the two trade unions and has made all the unions involved within ICI aware of how it is responding to the Act. Discussions have also taken place within the ICI joint consultative system, and as far as the company is aware these unions (and employees) are satisfied so far with its approach.

Acknowledgements to the editor of Industrial Relations Review and Report Bulletin: No 400 (September 15th 1987) for permission to reprint an edited version of Keith Holroyd's article, ICI: Data Protection (p.9). Published by Industrial Relations Services, 18 - 20 Highbury Place, London N5 1QP (Telephone: 01-354-5858).