RESPONDING TO ACCESS REQUESTS - HOW SHOULD EMPLOYERS COPE?

At the heart of every data protection law lies the right given to data subjects to gain access to records held on them. Companies should review their access procedures in countries with new data protection laws, and those which will soon pass laws, and even look again at their procedures in countries with well-established privacy laws. A survey by Industrial Relations Review and Report studied data subject access policies in some 40 companies as the UK law was coming fully into force. Although this survey relates to the UK, the lessons to be learnt about how employers can best cope with the challenge of employee access apply universally.

For many companies, the data subjects about which they have most immediate concern are their employees. This group is most likely to feel threatened by inaccurate data, as it could affect their career prospects, and they are best placed to know how to exercise their rights of access within their company.

The self-selecting nature of such a survey, means that all the organisations had already gone some way towards preparing for the introduction of subject access rights, and may give the misleading impression that many companies are as fully prepared as these. This, according to the Data Protection Registrar, is not the case.

One important general conclusion from the survey is that the changes required to existing practices of disclosure or non-disclosure generally flow from the organisation's management style and from the procedures in use to manage employee data.

Current Practice

27 of the 40 organisations surveyed have an existing policy of openness, and 17 of the 27 disclose some data at more or less regular intervals without prompting. Provision of information as a routine procedure combines the merits of openness with the practical benefits of allowing verification by the employee that the data held remains accurate. For example, Book Club Associates provides a "personal details check" every six months covering basic facts. Employees endorse or amend the information before returning the file to personnel. At Geest, the unprompted disclosure of information that occurs from time to time will now be formalised into an annual disclosure.

Publicising the new rights

Employers are under no obligation to inform their staff of their rights under the law to gain access to personal information. More than any other type, personnel and employee administration data occurs with the most frequency amongst the purposes registered by data users. It follows that publicity initiated by an employer and the involvement of representative staff bodies will therefore become highly effective avenues for alerting individuals to their new rights. Dun and Bradstreet have distributed a glossy leaflet which states clearly, for example: "The subject of personal data is entitled to a complete copy in everday language of all the information held in computer systems about them." BASF UK featured access rights in a 20

minute item in a large management seminar and in a staff journal article. Several internal company newsletters, like those of American Express and Spillers have featured employees' data protection rights.

Trade Union Involvement

The survey finds that trade union involvement in data protection protection is, surprisingly, at a very low level. Amongst the 40 organisations surveyed, there was only one formal management-union agreement (London Borough of Haringey) and one draft negotiation (Lothian Regional Council in Scotland). Others known about are largely within the engineering sector, and frequently involve APEX. Agreements exist at Ford, Rolls-Royce, Swan-Hunter Shipbuilders, and at Howells Motors.

Which data is covered by the law?

Manual files of personal information are entirely outside the UK Data Protection Act. Computerised files falling within the legal definition of "personal data" are covered by the law, i.e. all information, facts and opinions about an identifiable, living individual. The main exclusions cover:

1. data of a collective nature covering more than one individual, or used for statistical, payroll and research purposes.

2. information which concerns intentions towards the individual concerned.

In practice it is often very difficult to distinguish between opinions and intentions, particularly in personnel and career planning areas where job evaluation and performance assessment are concerned. Both the way the information is recorded and the way in which it is used by the data user will be relevant. Several organizations in the survey have overcome the problem of distinguishing between opinions and intentions by giving employees access to both categories of records. In due course, judicial interpretation will be necessary to resolve these anomalies.

Disclosure of sensitive information

The survey revealed that nearly half of those companies questioned intended to reveal more than the statutory minimum, and even inform employees of the full range of data that is kept on them even where disclosure is not required. Payroll and pension records are by far the most likely categories to be open to disclosure. But about one in five of the companies questioned indicated that they would be prepared to disclose information from other categories, such as disciplinary and performance/appraisal records held manually and comments relating to management's intentions towards the employee. Companies giving access to one or more of these categories include Nabisco, Procter and Gamble and Dun & Bradstreet. Some companies will be disclosing nothing beyond the legal minimum e.g. Swan Housewares, Penguin Books and Spillers Foods.

Only one company had indicated that some sensitive data will be transferred from disclosable computer to non-disclosable manual files. But, common practice is that the more sensitive employee records are manual files anyway. Only one company has revised its storage time for personal data as a

result of the Act - BASF UK intends to revise the length of time that disciplinary records are held prior to erasure.

Where trade unions negotiate an agreement, they have so far covered both automated and manual data.

Requesting and locating data

The data subject requesting to see personal data must do so in writing and enclose any stipulated fee up to the £10.00 legal maximum. Legally there is no insistence on the use of an application form; in practice it has proved helpful to the data subject because it indicates what is required, whether a fee should be enclosed and further details necessary for locating the data and to whom the request should be sent. From a management point of view, a standard form will assist in record keeping. Although forms can act as a deterrent, two out of every three organisations surveyed said that they would be making assistance available to help data subjects where necessary.

Data users have the twin legal obligations of preventing unauthorized disclosure of personal data, and of not unreasonably refusing to disclose data to the data subject concerned. The Registrar's guidance suggests that for non-sensitive data a signature would be sufficient proof of identity, but in the case of sensitive data further proof such as a national insurance number, date of birth or a witness to the signature application might be appropriate.

Fees and third party consent

A large majority of companies will charge no fee for employees to see their files, and most do not distinguish between current and former employees. Some employers are retaining the option to charge where access requests are greater than had been anticipated (Flavel Leisure, Bath City Council).

Releasing accurate data

The main conclusions on procedures for releasing data and ensuring its accuracy are;

1. Although legally required only to make data "intelligible," many employers will offer assistance to employees.

2. There is often standard guidance e.g. keys to file codes.

3. Only public sector organisations have so far taken steps to provide specific assistance to ethnic minorities, like information in minority languages.

4. More than half the organisations surveyed disclose data routinely, unprompted and with no fee. Many of these had done so before the Act came into force.

5. Additional accuracy controls had been found to be necessary.

6. Employees may need to confirm accuracy of data if it is based on information given by others, particularly in the area of monitoring ethnic origins or disability.

7. Many organisations had special internal procedures to handle data access complaints.

Making data "intelligible"

The Registrar interprets this as requiring terms to be understood by individuals outside the data-holding organisation generally, but not necessarily be understood by the data subject without assistance. Around 24 of the 40 organisations surveyed are making one or more members of staff available to help, although there is no legal requirement to do so. Almost invariably data is held in English, and translation for the benefit of ethnic minorities will cause major problems. Only four organisations questioned had contemplated providing translating assistance - all in local government. Of course if an outside agency has to be called in to translate the data, it will amount to unauthorized disclosure under the Act, with consequent liability for paying compensation to the data subject!

Organizations taking initiatives to release data

More than half the companies surveyed take the initiative in disclosing name-linked data to their personnel and most of these tend to do so annually. This procedure has several advantages:

1. Automatic disclosure is the most efficient means of maintaining accuracy and completeness of personnel records, particularly when an effort is made to ensure that employees inform record keepers of any errors.

2. Giving employees (and other data subjects like customers) an annual opportunity to check their records provides an organization with a defence in law (in the UK) against claims for compensation for damage and associated distress caused by inaccurate name-linked data.

3. Routine disclosure also provides opportunities for scheduling the task of preparing printouts for individuals to avoid workload peaks.

But it is unclear at present to what extent regular disclosure can replace access requests originated by employees. However, in contrast to the perceived advantages of unprompted disclosure, an organisation's security may be threatened by widescale dissemination of personal information due to the sheer volume of material!

Verifying and correcting

Data supplied after an access request has been made must be in its uncorrected form, but it is acceptable, perhaps even advisable for the organisation to indicate that errors have been detected and will be corrected after disclosure. It is obviously unlawful to change data in a file in the knowledge that an access request has been made; nor are changes to data permitted which are no part of a set routine. However, routine updating, deletion or amendment of data can continue to occur even if this means that a file could be substantially altered between the receipt of an access request

and its fulfilment.

Monitoring the work force

Where companies have monitoring programmes, for example, to give special training to minority groups, errors can occur if assessments are made by managers. As a result, eight organizations in the survey which monitor employees in this way, confirm the accuracy of such details with their employees.

Internal complaints procedures

In cases where an organisation refuses to make a correction to data requested by a data subject, he may either begin court proceedings, or make a complaint to the Data Protection Registrar, which involves no cost. However, two-thirds of organisations surveyed have tried to ensure that these sanctions are only a last resort. They have established a special complaints procedure for their employees at which data protection problems can be discussed informally. Where this route does not exist, an existing grievance procedure will provide an alternative channel for the resolution of disputes.

Summary

1. The public, according to the Data Protection Registrar's research, values data protection very highly, and would like to extend its principles to manual as well as computer records.

2. Many organisations take the law only as a starting point for a policy of open access together with overall data security.

3. Trade unions and staff bodies have had only limited impact on company data protection policy.

4. The interest in employees gaining access to records on themselves has been less than some companies expected. A major scandal would undoubtedly arouse much greater interest. Meanwhile, the common practice of regular unprompted disclosure may satisfy latent public curiosity.

5. Probably many data users have made little preparation for coping with access requests. But the Data Protection Registrar's publicity, together with media coverage of any prosecutions of companies which do not give their data subjects the rights to which they are entitled, will be a powerful stimulant to action. These factors will probably encourage companies which have not yet done so to adopt those access policies outlined here which comply with the letter and spirit of the law.

PL&B gratefully acknowledges the editor's permission to produce this edited version of the survey reports published in Industrial Relations Review and Report nos. 402 and 404, 13th October 1987 and 17th November 1987. Published by Eclipse Publications Ltd, Industrial Relations Services, 18-20 Highbury Place, London N5 1QP, Telephone: 01-354-5858.