The Data Protection Act (1998) Management Guidelines

Introduction

The Data Protection Act 1998 requires organisations to process personal data fairly and lawfully and in accordance with principles contained within the Act. The Act covers both paper based as well as computerised records. The personal data included under the Act are all filed records that are subject to processing, this means any records that are filed, altered, used, disclosed, erased, destroyed, stored or recorded.

Under the Act the employee has the right to inspect any relevant records, obtain copies and to challenge any inaccuracies contained in the records. The Act also imposes controls on the type of information that an employer can hold about an employee and the conditions that must be satisfied before specific types of information can be held.

The only exception is that until 23rd October 2007 records processed before 24th October 1998 may be requested by individual employees but there is no right to demand ratification of this data.

Storage of Personnel Records

The following records should be held on personnel files and retained throughout employment and for six years after the end of employment:

- Application Form / CV other related recruitment documents;
- Signing on Form (if appropriate);
- One or two copy documents proving eligibility to work within the UK;
- Statement of main terms and conditions;
- E mails - paper copies of e mails relevant to the employment. See the e-mail policy;
- Record of any amendments to terms and conditions;
- Change and additions forms (if appropriate);
- Medical questionnaires - retained in a sealed envelope marked 'Strictly Private & Confidential - Employee Name - To be opened only by Medical Records Administrator;
- Investigation and disciplinary documentation - spent warnings should be removed;
- Grievance records;
- Next of kin details;
- Authority to Drive forms;
- Sick absence documents;
- Appraisal documents;
- Training records;
- Letter of resignation and copy exit documents;
- Third party documents; and
- Employment references - not to be accessed by employee.

Procedure for Dealing with Employee Request

A request from an employee to see personal data held by the Company must be made in writing and a fee of £10 paid. This request must be specific about the information the employee wants to see as it is unreasonable for the employee to ask for all the information held. The person responsible for the data should then check the employee record to make sure it meets the standard set out below. The employee is then entitled:

- to be informed whether personal data are being processed;
- what the data are, why it is being processed, and to whom it has been disclosed;
- to be shown data, and to be told usually in writing the source; and
- to be told of the logic involved in decision taking where there is automatic processing of data (e.g. computerised recruitment selection).

The employee is not entitled to see employment references provided to the Company from past employers, or to see information used for management planning, proposed redundancy plans or organisational restructuring plans.

Employment References

There is no legal obligation to provide a reference. If however a reference is given it should be produced from one single source in the Company to ensure consistency. All references must:

- be headed up 'in confidence';
- indicate whether personal knowledge of the individual is known;
- refer to the facts known to both the employer and employee;
- only respond to the questions that have been asked; and
- refer to objective facts rather than personal opinion.

References must not:

- include new information that has not been discussed with the subject of the reference enquiry; or
- be economical with the truth.

Employer Responsibility

Those who have responsibility for employee records should ensure that:

- all data is accurate and up to date;
- errors are corrected promptly, making sure the corrections are passed to others who may have been given inaccurate data;
- data is deleted or destroyed when they are no longer needed;
- data is stored securely, and extreme care is taken to prevent unauthorised access;
- no more data than needed is recorded;
- personal data is not used for a purpose other than that for which they are collected; and

- sensitive data is not recorded unless there is explicit consent from the data subject.

Employee Rights

Employees have a number of rights under the Act, including the right:

- to be given written details of the processing of information relating to them;
- to prevent processing likely to cause substantial unwarranted damage or distress;
- to seek compensation if loss or damage is suffered by reason of a breach of the Act; and
- to have inaccurate data corrected or deleted, and if not complied with, the right to seek correction of information through the civil courts.

Employee Responsibilities

It is the employee's responsibility to:

- keep the line manager informed of any changes to personal details; and
- inform the next of kin that their personal details (i.e. name, telephone number etc) may be held on a personal file.

Processing

Under the Data Protection Act data can be processed as long as they are:

- processed fairly and lawfully;
- obtained for specific lawful purposes and not used in any way that is incompatible with those purposes;
- adequate, relevant and not excessive;
- accurate and up to date;
- kept for no longer than is necessary;
- processed in accordance with the data subject's rights;
- kept secure; and
- is transferred only to countries that offer adequate protection.

Types of Data

Personal Data

At least one of the following conditions must be met to allow the processing of personal data:

- the individual's consent has been obtained (all new recruitment documents include the necessary statement);
- it is for the performance of the employment contract;
- it is to discharge Company legal obligations;
- it protects the interest of individuals, e.g. their medical allergies and any emergency treatment

required;

- it is necessary for the administration of justice; and
- it is necessary for the legitimate interest of an employer, e.g. for processing payroll.

Personal Data will include:

- date of birth;
- marital status;
- next of kin;
- address;
- appraisal information; and
- medical history etc.

Sensitive Data

There are different conditions that should be met before processing sensitive data:

- explicit individual consent has been given;
- the performance of the employment contract is not possible;
- where consent cannot be given the protecting of the vital interests of the individual is necessary;
- it is carried out for legitimate activities relating to political, philosophical or trade union purposes which relates to individuals who are members of that body;
- the individual has already made the information public;
- it is necessary for medical reasons and is to be used by a health professional; and
- it is processed as part of an equal opportunities survey audit.

Sensitive Data will include:

- racial information;
- ethnic origin information;
- political opinions;
- health information;
- sexual life;
- trade union membership; and
- criminal offences.