



# DATA PROTECTION ACT, 1988

Procedure No: 34  
Revision: 1  
Sheet of : 1 of 4  
Date of Issue:  
January, 2001

## 1. **PURPOSE**

To define procedures in relation to Data Protection.

## 2. **SCOPE**

This Act ratified the Council of Europe Convention on Data Protection, and regulates the collection, processing, keeping, use and disclosure of personal information that is processed by automated means.

### **Scope**

- All employers
- All employees

## 3. **DEFINITION OF TERMS**

**Data:** Information in a form in which it can be processed (automatically). The Act applies whether or not the personal data are kept on mainframes, minicomputers, microcomputers, or word processors. The Act does not apply to data, which is held on manual files.

**Data Controller:** Person who controls the contents and use of personal data. A data controller can be a person, a firm or a corporate or unincorporated body.

**Data processor:** Person who processes personal data on behalf of a data controller. It does not include an employee of a data controller who processes such data in the course of his/her employment.

**Data subject:** An individual who is the subject of personal data.

*Personal Data:* Data relating to a living individual (not a company) who can be identified either from the data or from the data in conjunction with other information in the possession of the data controller. Such personal information could include data on an employee's health, family and social circumstances, political opinions etc.

Certain data will be exempt from the terms of the Act. These relate to data kept for the purpose of safeguarding the State, data required by law to be made available to the public, data kept by the individual and concerned only with his/her personal, family or household affairs or for recreational reasons.

#### 4. **KEY PROVISIONS**

The Act gives a right to every individual, irrespective of nationality or residence, to establish the existence of personal data, to have access to any such data relating to him/her and to have inaccurate data rectified or erased.

It imposes obligations on data controllers and data processors to ensure that automated data kept are accurate, up to date, and are kept for lawful purposes; that due security measures are taken; and that data are not disclosed for any reason incompatible with the purpose for which they are kept.

#### 5. **THE DATA PROTECTION COMMISSIONER**

A Data Protection Commissioner has been appointed under the Act to supervise the operation of the legislation and to investigate complaints.

Certain categories of data controllers and data processors are required to register with the Data Protection Commissioner. These are:-

- all Public Authorities
- all financial institutions, life assurance and insurance companies, or businesses, which are wholly or mainly involved in direct marketing, credit referencing or collecting debts
- data controllers who keep personal data relating to racial origin, political opinions, religious or other beliefs, physical or mental health, sexual life, or criminal convictions, collectively called sensitive data

- data processors whose business consists wholly or partly of processing personal data on behalf of data controllers, for example computer bureaux
- Finally, data controllers or data processors who may be prescribed under the Act by the Data Protection Commissioner with the consent of the Minister for Justice. To date, no such prescription orders have been made.

**Note:** Therefore, if an employer, as such, does not fall within the above categories, s/he is not obliged under the Act to register with the Data Protection Commissioner.

*Companies which keep ordinary personal data relating to employees including such matters as absence/injury records, disciplinary records, etc., are not required to register simply by reason of keeping that data. Such matters are not sensitive within the meaning of the Act.*

## 6. DUTIES OF DATA CONTROLLER

Data controllers must abide by what are known as the Data Protection Principles.

There are seven in all and they are as follows:

- *The "fairly obtaining and processing" principle*

An employee should be told why the information is needed, should be given an explanation of what use such information may be put to and the information should not be used for any other purpose.

- *The data shall be accurate and kept up-to-date*

The employer must take care to keep data accurate and up-to-date because if they are inaccurate or not kept up-to-date, they may cause damage to the individual concerned who is most likely to be the employee. The Act extends the law of tort by specifically imposing a duty of care on data controllers and processors.

- *The data shall be kept for specified and lawful purposes*

This means that if the data are kept for some other purposes, a complaint to and an investigation by the Data Protection Commissioner, may result in prosecution under the Act.

- *The data will not be used or disclosed in any manner incompatible with those purposes*

For instance, it would appear that data collected and kept on employees for personnel administration reasons, should not be used for direct mailing unless specified for this purpose in advance.

- *The data must be adequate, relevant and not excessive in relation to that purpose*

In other words, the data kept must be in proportion to the use to which they are put. Therefore, some personal details may be quite irrelevant or may be excessive under this rule. This is a matter of judgment and is related to the next principle.

- *The data must not be kept for longer than is necessary*

At some stage, data will become stale or irrelevant, for example, the fact that your employee may have received a criminal conviction 15 years ago, may be of no relevance at the present time for the purpose for which the data is kept.

- *The security principle*

Data controllers and processors are required by the Act to initiate and maintain appropriate security against unauthorised access to, alteration, disclosure or destruction of personal data and against accidental loss or destruction. Examples of such security requirements would be the use of code words, passwords, restricting physical access. The first 6 principles apply to data controllers only, whereas the security principle applies to both data controllers and data processors.

## 7. DUTIES OF DATA PROCESSORS

The only provision that applies to data processors is that requiring appropriate security measures to be taken in relating to the data. It is an offence for a data processor knowingly to disclose personal data without the prior authority of the data controller on whose behalf the data are processed.

## 8. DUTY OF CARE

The Act imposes on all data controllers and data processors a duty of care towards data subject to the extent that such a duty does not already exist under the law of tort.