KT

PERSONAL DATA PROTECTION

Legal obligations in respect of privacy and data protection are currently of great interest and importance to company managers, employees and the general public. The UK Data Protection Act 1984 is directed towards the protection of computer-based personal data, defined as "data consisting of information which relates to a living individual who can be identified from the information". This definition allows little scope for compromise. It applies to *you*, and must be taken into account when planning or using computer systems.

This book describes factors which contribute to the protection of personal data on computer files. Legal and practical aspects are considered, and the book shows how data protection can improve, rather than inhibit, the use of computer systems. The author examines how data protection requirements may be built into all stages of system development or acquisition, and into the operational use of computers. Although written largely from the point of view of commercial organisations, the topics are relevant to *all* users of computer systems storing financial, personal or other types of sensitive data.

John Court, Secretary of the IT Group of the Institute of Chartered Accountants, is a member of NCC's panel of computer audit lecturers. He has written a number of articles and papers on information technology, computer auditing and data protection.

NCC THE NATIONAL CENTRE FOR INFORMATION TECHNOLOGY

NCC Publications

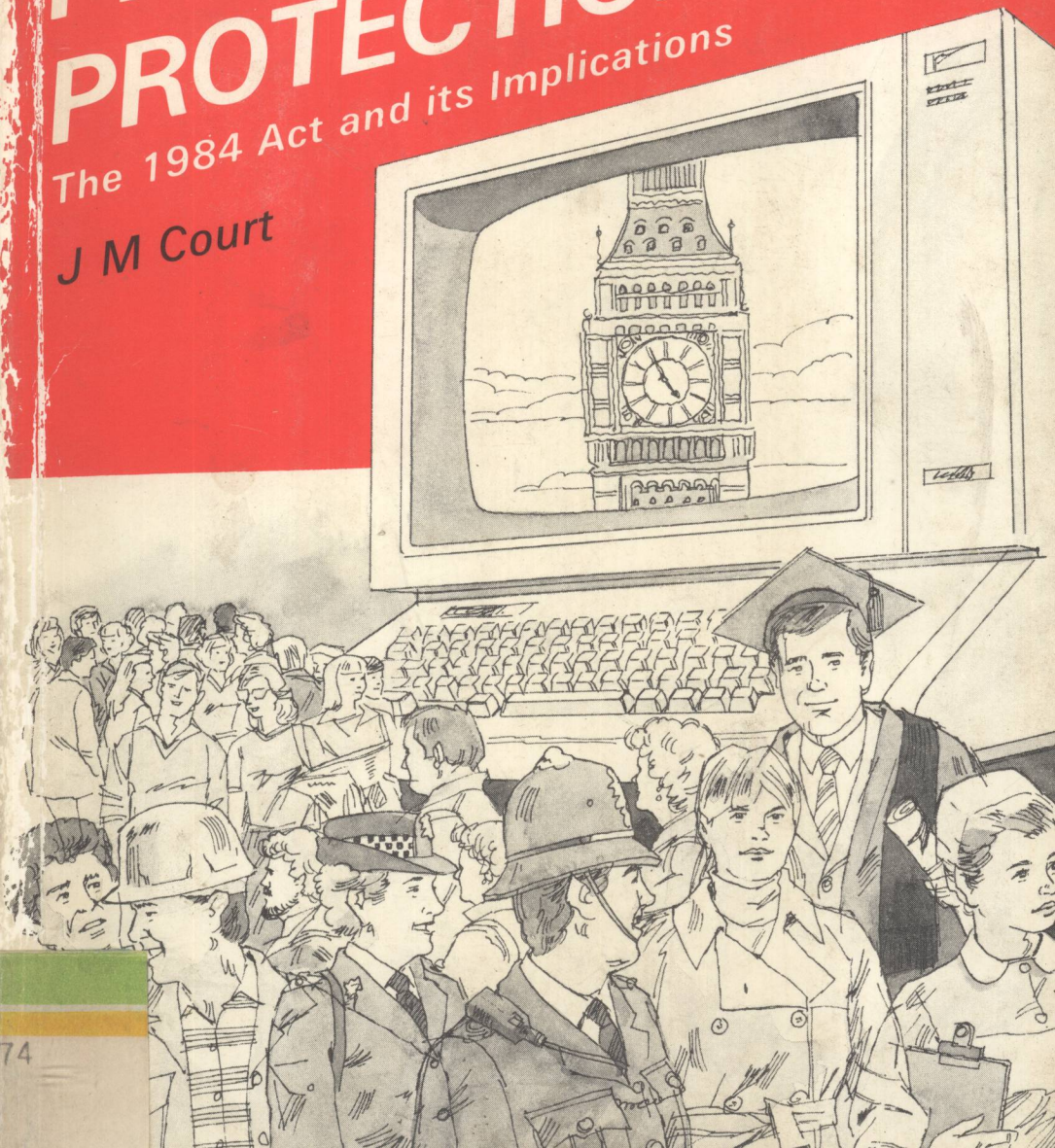
ISBN 0 85012 424 7

NCC PUBLICATIONS

PERSONAL DATA PROTECTION

The 1984 Act and its Implications

J M Court



Personal Data Protection

The 1984 Act and its Implications

J M Court

PUBLISHED BY NCC PUBLICATIONS

First published in 1984 by:

NCC Publications, The National Computing Centre Ltd, Oxford Road, Manchester M1 7ED, England.

Typeset in 11pt Times Roman by UPS Blackburn Ltd, 76-80 Northgate, Blackburn, Lancashire; and printed by Hobbs the Printers of Southampton.

ISBN 0-85012-424-7

Contents

		Page
1	**Introduction**	7
2	**The Legal Framework**	9
3	**Legal Obligations**	13
4	**Who Uses Data and Why**	19
5	**Data-Protection Principles**	25
6	**Data-Protection Procedures**	33
7	**Protecting Special Types of Data**	59
8	**Mitigating the Effects of Legislation**	67
Bibliography		71
Index		73

1 Introduction

This book describes the factors which contribute to the protection of financial data on computer files, and explores the extent to which these factors also contribute to the protection of personal data in computing, word processing and other information technology systems. Other aspects of personal data protection are also examined in detail, in relation to legal and other requirements.

The scope and impact of data protection law are examined, but the book is not confined to a discussion of legislation. It also considers what is important in general in data protection and what is important in particular in relation to all categories of sensitive data (including personal data, financial data, etc).

The book also shows how data protection can assist and improve, rather than inhibit, the use of computer systems. It examines how requirements for data protection may be built into all stages of system development or acquisition, and into the operational use of computers. The need to integrate manual procedures with the use of computer systems is not overlooked.

The following chapters are written largely from the point of view of commercial organisations, but this is only for convenience. The matters considered are applicable, mutatis mutandis, to *all* users of computer systems holding personal or other sensitive or valuable data.

Section numbers quoted in the text and in the footnotes are references to the Data Protection Act 1984.

2 The Legal Framework

INTRODUCTION – THE DATA PROTECTION ACT 1984

The Data Protection Act, finally enacted in 1984, is directed towards the protection of personal data (which it defines as "data consisting of information which relates to a living individual who can be identified from the information, or from that and other information in the possession of the data user"). This definition allows little scope for compromise.

The Data Protection law applies *only* to computer-based records. If records are maintained clerically they are completely outside the scope of this law.

The purpose of this legislation is stated as being:

(i) to implement the proposals set out in the White Paper on Data Protection published in April 1982 (Cmnd. 8539);

(ii) to enable the United Kingdom to ratify the European Convention (which the UK has signed) for the Protection of Individuals with regard to Automatic Processing of Personal Data.

Of these purposes (which in practical terms are more or less identical, since the White Paper incorporates the main features of the European Convention), the second is apparently regarded by the government as the more urgent.

The law establishes a Data Protection Registrar, who will maintain a register of personal data users and computer bureaux and have powers to ensure that personal data is used in accordance

with stated data protection principles. It sets up an Appeal Tribunal for data users; and gives data subjects certain legal rights, including a (sometimes qualified) right of access to their personal data, and in certain circumstances a right to compensation if such data is misused. We will return in due course to a detailed consideration of a number of these matters.

This legislation was first published as a Bill in December 1982. The publication of the Bill was something of an anti-climax, after two Committees of Enquiry and at least ten years of discussion about the need for, and the possible contents of, such legislation. This discussion involved such bodies as the National Computing Centre, the British Computer Society and the Institute of Data Processing Managers, as well as the legal profession, the medical profession, the police and civil liberties groups. Only after the Bill had been published did many people begin to realise that such legislation was actually possible – and reactions were mixed.

Many decision-makers and opinion-framers did not see the need for such legislation and resented the implication that they and their organisations were not responsible users of data. Also, many small business people found the prospect of such legislation (like that dealing with PAYE, VAT and statutory sick pay) irksome, and considered that they would almost certainly find it oppressive and time-consuming.

Both categories of people expressed opposition, forcing the government to change the scope of the legislation. The loss of the 1982 Bill because of the General Election of June 1983 did not really affect this process, but did make it possible for the Home Office to incorporate changes into a new version of the Bill which could then be introduced, with minimum embarrassment, into a new Parliament.

One of the changes made at this stage was that people keeping computerised records for accounting purposes were (generally speaking) exempted from any requirement to register as data users, or to allow the subjects of those records to have access to their contents. People using computers to calculate staff pay and pensions were similarly (generally speaking) exempted.

However, this issue is by no means as clear-cut as would have

been desirable. The use of personal data held for the purpose of calculating amounts payable by way of remuneration or pensions in respect of service in any employment or office is exempt from registration under the Act, and the subject of that data has no right of access to it. But this does not apply to personnel records – so if you use the same files both in your payroll calculations and in the maintenance of your personnel records this exemption, strictly speaking, *does not apply*.

This is almost bound to be the case if you use an integrated database – so the use of an integrated database for personnel records is almost bound to remove the exemption. Yet the use of such databases is growing more widely – so what price the exemption?

The same exemption is also available when data is used for the purpose of keeping accounts relating to any business or other activity conducted by the data user, or of keeping records of purchases, sales or other transactions. Again, if you use the same database of stock records for both accounting and other purposes (eg production control, stock control), or the same customers' database for both accounting and credit rating purposes, the exemption for accounting purposes is likely to be removed by the non-applicability of its exemption to the other purposes.

Further comments will be made on these matters in later chapters.

LEGAL REQUIREMENTS FOR GENERAL DATA PROTECTION

Many people resisted the whole idea of data protection, and exerted particular pressure to secure the exemption of accounting and payroll records. It was felt that there is already a framework of laws which protects business data in general and accounting records in particular. Such laws do not ensure the integrity of personal data specifically, or any element of data completely, but do together help to ensure that all data (including, therefore, personal data) is reasonably accurate and reasonably well-controlled. It is important not to underestimate the scope or importance of these general legal requirements (the most significant are considered below).

The Law of Libel

It is libellous to cause personal damage by publishing inaccurate information (for example, if you tell a debt collector that Mr. A has owed you £1,000 for the past six months, when in fact he paid you in advance, and Mr. A is financially or socially embarrassed as a result, Mr. A can sue you). Publication of inaccurate personal information as the output of a computer system is certainly within the scope of this law.

Forgeries, Theft or Unauthorised Release of Customers' Funds

If a bank pays over your money on the basis of a forged instrument, it must give you a refund. The same applies to the use of your cheque card, or credit card, if you have reported it missing as soon as you discover its loss. If the use of these facilities is connected with the operation of the bank's computer systems (as it normally is), the bank is under an obligation to its customers and shareholders. A sound system of internal controls over its customers' computer records (which in this case are both important personal data and significant accounting information) is required in order to minimise the chance of successful forgeries, thefts or unauthorised release of funds. Similar considerations apply to incorrect or unauthorised standing-order payments or direct debits.

Need for Audit of Limited Liability Company

All limited companies have to be audited by specifically qualified professional auditors. The auditors have to report on the truth and fairness of all sets of accounts showing the state of affairs of a company (its assets and liabilities), and its profit or loss for the period covered by the accounts. In coming to their conclusions on these matters, the auditors normally have to evaluate the company's systems of internal controls, including those which seek to maximise the security, confidentiality, accuracy and completeness of the company's computer records, in so far as these incorporate accounting records or records of assets or liabilities.

3 Legal Obligations

Apart from any of the matters to be discussed in later chapters, there are specific obligations under the Data Protection legislation to which you must pay attention if you hold any personal data for non-exempt purposes[1]:

— apply for registration as a data user within 6 months of the date fixed[2] by the Secretary of State for the law to come into force. You are not prohibited from processing any data until six months after this date, although from the outset you must observe the data protection principles set out in the Data Protection law (see Chapter 5). You are obliged to register:

  — your name and address;

  — a description of the personal data to be held by you and of the purpose or purposes for which the data is to be held or used;

  — a description of the source or sources from which you intend or may wish to obtain the data or the information to be contained in the data;

  — a description of any person or persons to whom you intend or may wish to disclose the data;

  — the names or a description of any countries or territories outside the United Kingdom to which you

[1] Exemptions are discussed in Chapter 7.

[2] Still to be fixed, following the enactment of the legislation. (Unfortunately, you will have to pay a fee.)

intend or may wish directly or indirectly to transfer the data;

— one or more addresses for the receipt of requests from data subjects for access to the data.

If you are *only* a computer bureau, you need *only* register your name and address, but you must *also* make sure that those who use your services are themselves properly registered as users.

You are deemed to run a "computer bureau" if you provide others with services in respect of data, either

— as agent for other persons[1] (ie you run computer systems on their behalf), or

— you allow other persons the use of your equipment to run their own computer systems.

If you *use* a computer bureau, you are still a data user and must register accordingly – ie you must register *all* of the above-mentioned details.

— do not process data, after registration (or after six months from the date to be fixed), except in accordance with the terms of your application to be registered. The Registrar cannot strike you off the register (by means of a "de-registration notice"), for any reason whatsoever, until 2 years have elapsed since the date fixed by the relevant Secretary of State (in this instance the Home Secretary); but

[1] In the opinion of the author, statutory auditors, performing computer audit techniques by processing their clients' files on their own (the auditors') computer, are operating as a computer bureau and should register accordingly. Correspondingly, clients may wish to register "audit" as one of the purposes for which personal data may be used (for example in payroll systems) – though for other reasons, to be mentioned later, this is not strictly necessary. After all, if the *client* is registered as the "user" of the data – in the sense of controlling it – then the *auditor* must be something different. In fact, the auditor *must not be* the user of the data in the sense of controlling it: an audit is conducted to discover whether or not the data is correct – not to control it.

  - he may seek to take action against you, subsequently, in the light of adverse information obtained about you during those 2 years;
  - even during these 2 years, he may impose specific requirements on you, or indicate an intention to strike you off the register, by means of an order taking effect at the conclusion of that period.

- do not transfer information, after registration, to another data user outside the UK except in accordance with the terms of your registration, and do not contravene the terms of any notice from the Registrar (a "transfer prohibition notice") which places restrictions on your right to do so. Again, the Registrar cannot make such a notice stick for 2 years from the date fixed by the Secretary of State, but it would be more prudent to observe the spirit rather than the letter if the Registrar serves such a notice, pending expiry of that period, at any earlier data.

- allow any applicant, on payment of the specified fee, to have full details of the data which you are holding about him/her[1]. Do not allow him/her to have access to any other data. You have 40 days in which to comply with a request for data access.

- do not allow anyone to have access to data about anyone else who has not consented to this[2]. This is an overriding principle: you can even refuse to allow an applicant to have access to his or her own personal data if this is impossible without inadvertently revealing someone else's. (But make sure it is actually impossible, not just inconvenient.) You must yourself be satisfied of the identity of a person who applies for access to personal data.

If you break any of these rules, the Registrar can issue an "enforcement notice", requiring you to comply with them.

[1] Again, provided you are not exempt from this requirement – see Chapter 7.

[2] Yet again, there are exemptions – see Chapter 7.

Renewal of registration will be required from time to time, probably every three years from the date of first registration. *Note particularly that* if the Registrar issues a de-registration notice and thus strikes you off the register, you commit a criminal offence if you continue to process any data by means of a computer system. This also applies if the Registrar refuses to register you in the first place (and still refuses to do so after the initial 2 years have elapsed since the date fixed by the Secretary of State), or if the Registrar refuses to re-register you.

You can appeal against any of these notices from the Registrar (ie de-registration notices, transfer prohibition notices and enforcement notices). Appeals must be made to the Data Protection Tribunal against any of these notices, or against a refusal by the Registrar to register you in the first place. The notices will all contain details of appeal rights.

The Data Protection Tribunal is a panel consisting of lawyers, computing specialists, computer users and laymen appointed by the Lord Chancellor and the Secretary of State. There is still a right of appeal from this Tribunal to the High Court (Court of Session in Scotland).

The Registrar's office, like all bureaucracies, will have a tendency to try to maximise its influence, and is therefore likely to put a strict construction on the meaning of "personal" and the scope of "personal data", and on the other requirements of the data protection law. In other words, you will not get away with non-compliance because your use of personal data is trivial or incidental, or because it is tedious to monitor your various uses of it. On the other hand, the Registrar will be responsible and reasonable in his enforcement of the provisions of the law, and will act with strict impartiality. For example, the Registrar will not take any action against you if you refuse to give someone (perhaps a disgruntled employee) access to some trivial item of personal data if it is quite clear that this person is not really interested in the data but just wants to cause you inconvenience.

The Registrar is the enforcement officer for the personal data protection law. Private individuals cannot seek to enforce the law. They can only seek damages against you in the civil courts. If you have caused them no damage then your non-compliance with the