SIXTH REPORT of the Data Protection Registrar June 1990

THE DATA PROTECTION REGISTRAR

LONDON : HMSO

SIXTH REPORT

of the

Data Protection Registrar

June 1990

Presented to Parliament pursuant to Section 36(5) of the Data Protection Act 1984

Ordered by The House of Commons *to be printed 17 July 1990*

LONDON: HMSO

£8.10 net

Contents

GENERAL INTRODUCTION

PART A: REPORT FOR THE YEAR

APPENDICES TO PART A

PART B: THE CORPORATE VIEW TO 1993

APPENDIX TO PART B

General Introduction

This Annual Report is in two parts. Part A reports for the year to 31 May 1990. Part B gives a Corporate View to 1993.

It has been a year of increasing volumes of activity and increasing complexity in the issues facing the Office. The Corporate View, which describes objectives, policies, activities, significant issues and finances, suggests that these trends will continue.

Part A: Report for the year

APPENDICES TO PART A

A1 Introduction

This part of the Report reviews activities for the year to 31 May 1990. It follows the same format as the Fifth Annual Report and the various sections broadly equate to the activities of the Office as described in the Corporate View.

There have been increases in the volume of work in virtually all activities. In addition, the range of data protection issues confronting the Office continues to grow. It has not been possible to cope adequately in this situation with the staff available. Steps are being taken to strengthen staffing but stresses are likely to continue for some time. Staff have responded well to pressure and I am grateful to them for their hard work, enthusiasm and positive outlook.

A2 Some Significant Issues

There are an increasing number of developments, in both the public and private sectors, which give rise to data protection concerns. Some are described in this section of the Report. Data protection issues may stem from new applications of computing, from new public policies, or from the advent of new technologies or techniques.

My staff must consider these developments carefully and determine how the requirements of the Data Protection Act apply to them. Computer users can then be informed and advised as to the requirements they must meet. Where appropriate, the powers given in the Act can also be invoked to ensure that the requirements are met.

It is clearly helpful to my Office and major data users, in both the public and private sectors, to have early discussions on new developments. Last year I said that I was pleased that a number of government departments were seeking views from my office at the early stages of development of new legislation or major computer applications which may involve the collection and use of personal data. This continues in some cases, but I am less sanguine about the situation as a whole.

I do not believe the Registrar should play a passive role in establishing early discussion of new developments. In so far as government departments are concerned, I am discussing with the Home Office the possibility of obtaining regular notification of the introduction of relevant legislation. I shall also seek to establish more regular contact with major private sector associations and computer users.

It is also incumbent on me to respond when approaches are made. I have to say that pressures on staff time have made responses by no means perfect. I hope that the new staff now being recruited will allow me to give faster and firmer responses from late this year onwards.

(a) The Construction and Use of Personal Identification Numbers (PINs)

In order to establish effective relationships between individuals and computer users it is necessary to identify and separate one individual from another. Good identification can have positive benefits both for individuals and computer users. On the other hand, attaching identity "labels" to individuals can give rise to privacy concerns. I have placed a discussion of personal identification numbers (PINs) in Appendix AA1 as an introduction to the issues which arise.

The wide availability and use of a PIN applied to individuals on a national basis facilitates "data matching". This technique involves searching through different computer files and, by use of a common identification system, extracting and drawing together from those files all the information held on a given individual. The files may be held by different computer users for unrelated purposes.

It is possible for a de facto common identifier to creep into existence and for this to have national coverage. The wider use of an existing identifier such as the national insurance number is not the only way in which this could occur; the same situation could arise from the encoding of information about individuals into PINs. For example, the use of a combination of name and date of birth to create a PIN, particularly if this were done to a common standard by multiple computer users and applied to a large proportion of the population, might lead to this situation.

More and more information about more and more individuals is being held on computer files. New and improved communications systems make electronic exchanges of information between computer users increasingly possible.In these circumstances and from the point of view of computer users, data matching becomes both more attractive and more feasible. We are likely to see an increasing interest in this technique.

However, data matching raises data protection concerns.It offers possibilities: for the wide use and disclosure of information without an individual's knowledge or consent; for the use of information out of context to the detriment of individuals; for the wide replication of errors by transferring any inaccurate information from one file to another; for unjust decisions about individuals simply on the basis of a "profile" which causes them to fall into a group with certain selected characteristics; for automatic decision making on facts of doubtful completeness, accuracy or relevance; for the surveillance of individuals; and for influencing peoples lives. There are now specific pieces of legislation or policies to guard against or control this activity in, for example, the United States, Canada and Australia.

There may be occasions where data matching can be used to further an important public policy, for example the prevention or detection of crime. These occasions and policies need to be considered in their own right along with the appropriate safeguards for individuals.

A Council of Europe working party has carried out a study into the structure and use of personal identification numbers and its report will be placed before the Committee of Ministers in September. The conclusions will provide helpful guidance. However, as will be seen in a number of issues considered below, problems concerned with identifying individuals are already with us.

In considering these issues, I should like to see the adoption of PINs which are "context specific" - that is, particular to a given computer user or a given use of personal data. It will help in achieving this if there is a presumption against information about individuals being encoded into PINs held by computer users. If circumstances dictate that it is essential to use information in that way, then there should be safeguards for individuals. It may be necessary to seek constraints and safeguards not only within the design and operation of the computer system itself, but in agreements, contractual or otherwise, governing the disclosure and use of the PINs and information in question.

(b) The Use of the National Insurance Number

Everybody is given a national insurance number at the age of sixteen. It therefore potentially offers itself as a form of national identifier, although, as its name suggests, it was intended only for use for a particular purpose.

However, there is no specific statutory restriction on the use of the national insurance number and over the last few years it has crept into use for other purposes. So far these purposes have lain in the public sector. The national insurance number is now, for example, the primary income tax reference number and its use has been extended into local authorities in connection with various

benefit payments. New legislation in connection with Personal Equity Plans (PEPs) constrains private sector organisations to collect national insurance numbers and this may portend the developing use of this number in the private sector.

As discussed in (a) above, the common use of a single personal identification number can facilitate the cross-matching of files of personal data. The decision by Ministers not to use the national insurance number for the Student Loans Scheme (see below) was therefore helpful. However, the general position on the use of this number and the policies for controlling that use is by no means clear. During the next year I hope to devote effort to examining this situation.

(c) The Student Loans Scheme

I was contacted about the Student Loans Scheme only in February 1990. This was late in the day and a number of decisions had already been taken on the computing system which is to be used. There are still many things to establish with the Student Loans Company, for example concerned with the fair obtaining of information and the length of time for which information will be held.

However, the key issue under discussion concerns the problem of identifying loan applicants and linking any particular applicant's records. The problem is heightened by the fact that loans must be made to any bona fide applicant; that those under eighteen are entitled to loans but such loans are not normally enforceable at law; that each student must make a new application each year for a separate loan; that loans in default but not repaid by certain ages are not recoverable; and that information will not be sought from credit reference agencies.

When the Department of Education and Science first approached my Office, the intention was to use the national insurance number as a student identifier. For the various reasons discussed above, I put the view that this was not desirable. Ministers supported this view and discussions then took place on other methods of identification.

In the event, the Student Loans Company is to use name, date and place of birth and sex, in order to link loan information on any given applicant. There will be specific safeguards to ensure the confidentiality of this information and its use only for the Student Loans Scheme. Referencing and linking of individuals by use of this information will be undertaken internally within the computer. The information will not be used to form a reference number for external access to loan information - that requirement will be met by allocating context specific loan numbers which will not contain encoded information about individuals. I note also that the Student Loans Company is prevented by statute from making information available to others for marketing purposes.

As will be seen in (d) below, I question the collection and use of date of birth by the consumer credit industry to assist in identifying individuals. The conditions under which the Student Loans Company will operate are not comparable with this industry. The Company is also offering helpful safeguards for individuals. Despite this, I have raised reservations about whether all the information to be used to identify individuals and provide the internal machine linkage will prove necessary. I have made clear that I will wish to review the matter formally after a period of three years. In the interim I expect my staff to stay closely in touch with the Students Loans Company to obtain the statistics necessary to assess the effectiveness and general applicability of the safeguards offered. The Student Loans Company has assured me that, if it proves possible to identify applicants satisfactorily without using all the items of information proposed, it will cease collecting and using the surplus items identified.

(d) The Consumer Credit Industry

(i) *Identifying Individuals*

The consumer credit industry has expressed a wish to collect more information in order better to identify individuals and link existing records to new credit applicants. However, this industry's position is different to that of the Student Loans Company: it has discretion over whether to give loans or not; it wishes to share its information between computer users; and it already has a sophisticated identity checking system available through the credit reference agencies.

In considering the position with regard to the consumer credit industry it is therefore appropriate to take account of the current situation and how this might be affected if information were to be collected, as proposed, not only on loan applicants' names and addresses but on their dates of birth also.

The credit reference agencies currently check and supply information to clients from three main files:

— a file of county court judgments which is compiled from information supplied by Registry Trust Ltd. This file has names and addresses of those who have been subject to county court judgments but it does not contain information on dates of birth. Entries on this file can be of very poor quality;

— a name and address file compiled from electoral registers which are purchased from Electoral Registration Officers. Electoral registers do not contain dates of birth, although it is possible to deduce the date of birth of an individual who is entered on a register on reaching eighteen years of age.

— a file of information provided by each of the members of a "club" of lenders. The information includes the names and addresses of individuals having loans with members of the club together with details of the loans and the payment records for them. Some of these records may contain dates of birth.

In the light of this, it is difficult to see where the use of dates of birth will improve the linking of records about a given individual, except perhaps in the case of those individuals whose ages are deduced from electoral registers, or whose records already contain date of birth when provided by the club of members.

Names and dates of birth could be used by lenders and the credit reference agencies to develop a common identifier containing coded information about individuals. In view of the nature of the credit reference industry (a widely available information service, with multiple users and files of information on virtually all the adult population), that could create the very circumstances which could lead to the wide use of this number as a de facto national identifier.

I will discuss with the credit industry any assessment which may have been made of the benefits, both for individuals and for lenders, which would flow from the collection and use of dates of birth to assist identification and record linkage. If, ultimately, it seems appropriate to use dates of birth in this way then I should be happy to consider, with the industry, appropriate safeguards for individuals.

(ii) *Looking to the Future*

In March I spoke to a conference organised by the Institute of Credit Management. The conference was concerned with credit developments during the "nineties". I took the opportunity to suggest that it would be valuable for discussions to begin now on credit assessment systems which might be in place in a few years time.

It seems sensible to look ahead in order to seek to avoid data protection problems in the future; because systems take a few years to specify and develop; because credit assessment systems seem certain to develop further; and because some of the possible lines of development are already becoming clearer. In addition, the run up to the open market in the European Community at the end of 1992 is likely to cause changes concerning both credit assessment and data protection, as a result of ideas from our European partners.

It seems to me that developments are likely to take place mainly through the "club of lender" schemes described above. The key problem will be to find a balance between the control which borrowers may exercise and the wish of lenders to exchange information through these multi-lender files. I do not see great problems with the storage of "black" (default) information though there may be issues about informing individuals when such information is passed to central reference files. Rather, it is in connection with the storage of "white" (positive, non-default) information that problems are likely to occur.

In continental Europe there is often reference to "informational self-determination", which I take to mean individual choice. The United Kingdom Data Protection Act does not use this term, although it does require information to be "fairly obtained". What is "fair" when obtaining data may vary from case to case, but the straws are already in the wind as far as an individual's right to opt out of secondary uses and disclosures of personal data are concerned. In the banking sector, the Government's response to the recommendations of the Review Committee on Banking Services Law (see (e) below) and a report recently prepared for the Council of Europe are supportive of such a right for individuals.

I have offered, through the credit industry's Forum on Data Protection, to talk about future credit reference systems and data protection requirements. I expect shortly to sketch out some first thoughts for discussion with the industry and with other interested bodies such as the Office of Fair Trading, the National Consumer Council and the Citizens Advice Bureaux.

(iii) *The Use of third Party Information in Credit Assessment*

I have commented on this issue in previous reports. I have taken the view that in so far as the systems employed by the credit reference agencies are designed to extract from their files information on one individual (a third party) in response to a request for information on another individual (a loan applicant) when that information does not relate to that applicant, then this amounts to unfair processing.

I have discussed this issue with the credit industry over a period of about two years. Last November, I concluded that these discussions were unlikely to resolve the problem and that I should consider formal enforcement action. Since then, my staff have drawn together all the supporting information in connection with formal enforcement and have sought leading counsel's advice on two occasions. After the end of the reporting year (31 May 1990), but whilst writing this report, I have had the opportunity to consider the reports prepared by my staff. That consideration has led me to serve Preliminary ("minded to") Notices on the four main credit reference agencies. The notices

presage enforcement action to cause these agencies to end the unfair processing associated with third party information. The agencies now have the opportunity to make representations to me as to why I should not go on to serve formal enforcement notices.

(e) Recommendations on Banking Services Law

The Review Committee on Banking Services Law reported in February 1989. The Committee proposed standards for obtaining, using and disclosing information on individuals which are very supportive of data protection objectives. They concerned, for example, the fair obtaining of information from individuals and practices for notifying individuals of their rights under the Data Protection Act.

The Government responded to the Committee's report through "Banking Services: Law and Practice", a White Paper published in March 1990. The Government's conclusions are also supportive of data protection objectives concluding, for example, that an individual should be able to opt out of the use of his or her banking information for marketing or credit reference purposes except, in the latter case, where black information is concerned.

The Government wished to see its conclusions introduced through a code of practice for banks and building societies. These organisations had already announced on 1 March 1990 that they were beginning work on such a code of practice and I look forward to being involved in discussions on this.

(f) Use of Information published under Statute

This subject is under discussion in a working party of the Council of Europe although no conclusions have yet been reached. There are difficult issues arising from the need to publish some information (eg. electoral registers) in order to protect the public and the problem of controlling the subsequent use of this information. It will be interesting to see what resolution of these issues may ultimately emerge from the Council of Europe.

During the year there was a change in respect of the supply of electoral registers for other than electoral purposes. The Representation of the People (Amendment) Regulations 1990 cause Electoral Registration Officers (EROs) to supply copies of their registers to anybody who places an order. Previously EROs only had to supply their registers for non-electoral uses if they chanced to have a spare copy and a number of EROs had effectively ceased to supply their registers for use for other purposes.

The Data Protection Act does not cover statutorily published information and therefore disclosures of electoral registers fall outside its provisions. But there are some actions which could be helpful to individuals in circumstances where they are, as in this case, effectively forced by statute to supply their names and addresses to those who care to buy these registers. I was disappointed that the position of individuals was weakened by these new regulations without any countervailing action to assist them.

The Home Office had previously ruled out the possibility of introducing a facility for individuals to opt out from the supply, of their details on electoral registers and confirmed this position in the parliamentary debate on the new regulations. However, it would be helpful if individuals could know to whom their information had been supplied. The information from the electoral registers will be subject to the Data Protection Act if it is held on computer by those who buy it. If individuals know who the purchasers are, they may be able to use their rights under the Act to check on the subsequent holding and use of their details.

Ministers have indicated that they will consider the possibility of EROs publishing, from time to time, a list of those who have bought their registers.

(g) The National Criminal Records System

The Home Affairs Committee of the House of Commons reported on the National Criminal Records System in April ("Criminal Records", Third Report of the Home Affairs Committee, HMSO).

The Committee carried out a short enquiry because of evidence about the failure to provide accurate criminal records to the Crown Prosecution Service and the courts. The Committee felt that the computerisation of these records would be likely to overcome some of the current difficulties. However, they felt that the change to a computerised system should be used as an opportunity to introduce a new consistency and fairness into the arrangements for the maintenance of criminal records. The Committee makes a number of recommendations to assist in achieving these goals. They cover issues such as the scope, nature and availability of the records as well as the methods for collecting and maintaining them.

I welcome the Committee's Report. It introduces a number of important issues into public debate. The timing is particularly appropriate in the light of the introduction of a new Police National Computer System (PNC2). I was pleased to be able to submit written evidence to the Committee and this is reproduced in Appendix AA2.

(h) The Community Charge

Community Charge Registration Officers (CCROs) began sending out forms seeking information for their Community Charge Registers in Summer 1989. That signalled the start of complaints to my Office about the content of these forms. It also heralded a year when I have had to put considerable resources into resolving the issues raised, to the detriment of other important work.

It is very disappointing that this turned out to be the case, for my staff had put a great deal of effort along with officials from the Department of the Environment and with the Local Authority Associations to give CCROs advice to avoid the kinds of problem which came to light.

In the event it proved necessary to obtain and examine the forms from all 403 local authorities. There were issues to be resolved on over 200 of the forms. The vast majority of the problems have been resolved by CCROs giving undertakings about their collection and use of personal data. However, as can be seen from Section A4 it has been necessary to refuse registration to fourteen CCROs and to issue enforcement notices against a further nine.

Problems have also arisen with some of the forms used by CCROs to update their registers. These seem to be fewer in number and it should not be necessary to repeat the major exercise just completed.

(i) Direct Marketing

Whilst the number of complaints about the receipt of unsolicited marketing literature has increased over the year, I believe that progress is being made in resolving a number of the data protection problems in this sector. This is because of action by particular organisations and by the Mailing Preference Service as well as through the efforts of my Office. That is not to say that the industry agrees with the view I have taken of the law.

My Office has mounted an extensive campaign to contact and advise organisations concerned with direct marketing to assist them with compliance with the eight Data Protection Principles. The specific targets have been: large data users in the direct marketing industry; large direct marketing agencies which advise numerous clients on this form of marketing; organisations involved with list broking and list rental; some representative bodies and charities.

A series of data protection seminars related to direct marketing are to be run, at five locations around the country, in October 1990. It is also planned to produce articles relating to data protection and direct marketing for the trade and technical press; the general press; and popular magazines.

The most significant issue for further investigation is direct mail from the United States and throughout Europe. This is a growing field and United Kingdom lists may be used extensively. The kind of protection offered by the Act may be unavailable once the list has left this country. This is an area of concern which is being examined. This is no easy task for there is a great deal to learn about the procedures and the market is expanding extremely rapidly.

(j) Human Fertilisation and Embryology Bill

The Human Fertilisation and Embryology Bill was introduced in Parliament during the year. It provides for the establishment of an authority, one of whose functions is the granting of licences to persons carrying out treatment services for the purposes of assisting women to carry children. The authority would establish a register containing information relating to the provision of treatment services, including information on, for example, persons receiving treatment, donors and children born as a result of treatment. The Bill envisages that the register would be held on computer, thus establishing a collection of personal data of a highly sensitive nature.

A number of data protection concerns arise, but the one which required the immediate attention of my staff was the question of the right of access of individuals to data relating to themselves on this register. I was concerned about the way in which the right of access was restricted in the Bill as originally drafted. It has always been my view that the general right of access under the Data Protection Act should be withdrawn only in exceptional circumstances. This is the approach which I adopted, for example, in discussions about access to personal health information.

I am pleased that the Department of Health was receptive to my views and that discussions between my staff and officials of the Department resulted in an agreed amendment to the Bill. The effect of this is that access to information showing that an identifiable individual was or may have been born as a result of treatment services is explicitly defined in the Bill rather than under the subject access provisions of the Data Protection Act. I expect to be consulted by the Department on the regulations which will define precisely what information is to be provided to such individuals.

(k) Codes of Practice

Work continues on encouraging the development of codes of practice. Developments during the year have included codes for:

- property management (Royal Institute of Chartered Surveyors, Incorporated Society of Valuers and Auctioneers and the National Association of Estate Agents);
- customer and supplier administration (Chartered Institute of Management Accountants, Institute of Internal Auditors and the Institute of Purchasing and Supply);

— computer bureau services (Computing Services Association);

— confidentiality of personal information (office of Population Censuses and Surveys);

— a revision of the code for direct marketing (the Advertising Association).

The first three of the above were developed by the National Computing Centre in association with the bodies named and with support from the Department of Trade and Industry.

In addition, codes are under development for the insurance and pensions industries and for pharmacists.

(l) Review of the Act

In the last Annual Report I gave the results of the review of the Act which followed a wide consultation with individuals and organisations. In addition to this review, an Interdepartmental Committee has been considering the working of the Act. I have acted as an adviser to this Committee which has recently completed its report and matters now await consideration by ministers.

(m) Other Issues Requiring Attention

— **The replacement Police National Computer System (PNC2).** With new staff coming into post in the next few months, I hope to give this more attention. The points raised by the Home Affairs Committee in respect of criminal records, reported above, will be taken up in this context.

— **Use of the Government Data Network.** It has now proved possible to schedule some work on this. The aim is to see if it is possible to analyse and describe any exchanges of data between different government departments and the policies and controls governing these.

— **Health Service Computing.** There are considerable developments planned for health service computing. With such sensitive data as medical records, it will be very important to see that data protection safeguards are fully in place.

— **The European Dimension.** Collaboration between European Community (EC) countries, for example with regard to policing and immigration control, are beginning to appear as the open market draws nearer. Data protection issues, including the question of equivalent legal positions in the various EC countries will generate activity and involvement for the Office.

— **Transborder Dataflows.** The first investigations into cases involving transborder data flows have taken place during this year. Whatever equivalent protection is established across the European Community this issue is increasingly likely to arise.

— **Personal Identification Systems.** As indicated earlier in this section, the problems associated with identifying individuals are arising more frequently. More work is needed to understand this subject as a whole so that appropriate guidance can be given to computer users.

— **Profiling Techniques.** The profiling of individuals is increasingly likely to be used, for example, for direct marketing using lifestyle databases, in credit scoring or in crime prevention. More work is required to assess the implications of these activities for the individuals concerned.

— **Data Matching.** A study is needed of the situations in which this is occurring, of possible future developments and of policies to control the use of this method of drawing together information on individuals.

A3 Complaints from Individuals

There has continued to be a sharp rise in the number of complaints received from individuals. I reported 1122 complaints for the year to 31 May 1989 and had expected this figure to rise by about 50% this year. In the event 2698 complaints have been received, a rise to almost two and a half times the previous year's total.

Generally speaking there has been an increase in the number of each type of complaint received, but the overall pattern of complaints has changed. Consumer credit complaints have fallen from 35% last year to 17% this; complaints that data users have not been complying with the subject access requirements have dropped from 18% to 8%. On the other hand, unsolicited mail complaints have risen from 16% last year to 45% this; and complaints that information has been unfairly obtained are now running at 15% of the total. A new feature has been the complaints concerned with the Community Charge. These have amounted to 7% of complaints received.

New methods of working have been introduced in order to speed up the handling of complaints. Staff from the complaints office have been trained in telephone techniques so that they now discuss complaints directly with complainants. This allows a quick assessment of the nature and seriousness of the complaint without becoming involved in protracted correspondence. Nevertheless, because of the increase in complaints, at the year end there were 310 complaints which it has not even been possible to look at, let alone progress. I am keeping this situation under close review and considering how this unacceptable backlog can be reduced.

With the new systems an early decision can also be made, where necessary, to task one of the regional investigating staff to interview the complainant and get a detailed statement of the circumstances of the complaint. This is an increasing part of the work of investigating staff along with the formal collection of information in connection with enforcement activities.

Some examples of complaints are:

Case 1

The complainant made a subject access request to a local council. On receipt of the computer print-out she became concerned about certain entries that were made about her mental condition. She had made attempts to have these entries amended but the council was not cooperative. After investigation of the complaint, the council changed the information on its files.

Case 2

The complainant purchased theatre tickets and paid by cheque. She was asked to provide her full name and address. These details were entered into a computer. The complainant was concerned about retention of these details in a computer.

The data user explained that the information was retained until the final performance of any production. It was deleted from the computer within four weeks after the final performance. The details were needed to identify the ownership of the seat in case of a dispute or to contact the owner of the seat in case of cancellation. The information was never passed to any third party.

The data user did not make individuals aware that details would be held on computer at the time of the purchase. However, as a result of the complaint the data user agreed to display a sign in the box office explaining the reason why the information was needed.

Case 3

The complainant wrote about inaccurate information on his credit reference file. In 1984 he had opened an account with a department store. In 1987 the complainant closed his account and made his final payment. The following year he was refused a credit card with another department store and as a result obtained a copy of his credit reference file. This showed his account with the previous store to be in default.

The first store had taken over responsibility for administering its own accounts from a banking organisation in 1987. It was not obvious which organisation had passed on inaccurate information to the credit reference agency.

Although the store was unable to pinpoint exactly where the error occurred it accepted responsibility for the error and offered the complainant compensation for the inconvenience he had suffered.

Case 4

The complainant was receiving reminders to renew a television licence. These were addressed to a lady with a similar name, but different address from his. He had approached the licensing authority three times but had been unable to resolve the matter himself.

It transpired that when the complainant renewed his licence the hand written document completed at his post office did not state the name of the district in which he lived, or the post code. The form was therefore referred to his local head post office which had then supplied incorrect information relating to his name and address. The licensing authority amended its records and removed the incorrect details from its files.

Case 5

A local council rates office had disclosed the complainant's address to her ex-husband. The complainant was divorced and had moved several times in an effort to prevent her ex-husband from contacting her. The ex-husband had informed the rates office that he was a relative and produced evidence proving his identity. It is normally the policy of the rates office to forward correspondence in these circumstances, but in this case, the clerk returned the envelope with the ex-wife's address.

The council's Data Protection Register entry covered the disclosure to relatives of ratepayers, but the council's own code of practice had been contravened. As a result of the complaint written instructions were re-issued to all members of staff reminding them that under no circumstances must information be disclosed to third parties; such breaches would result in disciplinary action.

Case 6

The complainant had noticed that the VDU screens in a hotel were positioned in such a way that anyone in the reception area could view their contents. The Financial Controller of the hotel initiated an internal enquiry and recommended that the position of the VDU screens be altered.

Case 7

The complainant received a questionnaire from the health research unit of a university. It related to a condition from which the complainant suffers.

The health research unit had written to all general practitioners in a particular geographical area seeking permission to look at prescription forms issued by them. The purpose was to identify patients who may have the condition in question and seek the GP's permission to send questionnaires to them. This process was completed manually and the information is not covered by the Data Protection Act. The information collected from the questionnaires will eventually be put onto computer but in an anonymous form.

Case 8

The complainant made a subject access request to a large database company and was informed that no data were held about him. A few days later he received a mailing from the same company.

The company stated that when the subject access request was received from the complainant no data were held relating to him. However, a few days later, personal data taken from a share register were input on to their system and this accounted for the mailing the complainant received. The complainant requested that his details be suppressed by the database company and this was arranged.

Case 9

The complainant was receiving large amounts of unsolicited mail addressed to his late wife.

The complainant was recommended to register his late wife's details with the Mailing Preference Service. He was also asked to send all the mail he received, addressed to his late wife, to the Registrar's office. After approaching all the organisations concerned and tracing relevant mailing list owners, it was possible to suppress the use of details about his late wife.

Case 10

A couple complained about mailings received from timeshare companies. All the timeshare companies were approached to ensure suppression of the couple's details. The complainants' details were traced back to three major database companies which supply personal data to third parties. These companies also confirmed that the complainants' details would be suppressed on their lists.

Case 11

The complainant answered an advertisement (in a journal) to receive more information on the products of a large publishing company. Included in the response letter was a clause which referred to the fact that details about the complainant would be used for direct mail purposes. The complainant objected to his details being passed to third parties and asked that his details be suppressed.

The publishing company was advised of the "fair obtaining" requirements of the First Data Protection Principle, particularly emphasizing that any notification of secondary uses and disclosures should appear at the point that personal data are obtained.

The publishing company decided to suspend its trading in personal data. The company considered that a notification clause would have an adverse effect on the response rate which would damage the sales of its main product.

Case 12

The complainant had submitted a subject access request to a large mail order company and had received no response. The organisation stated that the subject access request was overlooked whilst attending to the redirection of goods incorrectly delivered to the complainant's address. Staff have now been reminded of the need to study correspondence carefully for references to the Data Protection Act.

Case 13

The complainant had been suspected of using a stolen credit card when attempting to make a purchase at a large store.

The credit card company admitted that the error had occurred due to maladministration and offered some compensation to the complainant. The inaccurate data were corrected.

Case 14

The complainant sent in a building society computer print-out containing personal data which she had found discarded near her home. The officers of the society took the breach of security very seriously and quickly introduced new procedures for the disposal of confidential waste.

Case 15

The complainant had not received an adequate explanation of the codes used by a sporting authority on its files to make his subject access reply meaningful. Follow-up correspondence had been unsuccessful.

The full key to the coded records was obtained from the authority which was reminded of its obligations under the Act. The authority stated that it had attempted to explain the details by telephone to the complainant.

Case 16

The address relating to the complainant's bank account was amended by his bankers following instruction from his former wife. The bank stated that the complainant's ex-wife had advised them in writing of her change in marital status. This had been misinterpreted as a change of address request. A joint mandate existed on the account at this time. On receiving instructions from the complainant the appropriate correction was made.

Case 17

Complaints were received concerning a letter sent by a theatre company to individuals on its mailing list. This letter informed individuals who had not paid

their subscriptions, or had allowed them to lapse, that their names had been rented out to other organisations. It went on to say that one of these companies had copied the list onto its database and that the theatre company therefore had no control over the mailings that might be sent as a result.

Inspection of the Data Protection Register revealed that the company was not registered to hold or obtain personal data about prospective theatre goers, to use such data for marketing purposes or to disclose such data to other theatre companies.

The theatre company was prosecuted for four offences under Section 5 (2) of the Data Protection Act.

Case 18

The complainant had been negotiating to sell his house. The sale fell through, but the prospective purchaser had given the address as a forwarding address to an organisation for which he had an outstanding debt. This organisation filed details of the debt with a credit reference agency under the complainant's address. The agency agreed to delete details of the debt.

Case 19

The complainant was concerned that information concerning his account with a building society had been disclosed to his wife. This information had been sent to his address in an envelope addressed to his wife.

The building society admitted the breach of security, which was due to an administrative mix-up involving the complainant's two accounts, one of which was held jointly with his wife.

Procedures were in place to avoid this kind of error, but an individual cashier had not followed these procedures in this case. The society gave assurances that the procedures had been amended and that all staff were to receive continual reminders of the necessity to follow these procedures to the letter.

Case 20

The complainant continued to receive requests for payment from a mail order book company despite having paid all outstanding monies. His cheque to the company, for the amount specified in the continuing invoices, had been cashed.

The company admitted that the complainant had been recorded on its database as being in debt to the company. The company confirmed that the account was now clear and no record of the alleged debt had been retained or passed on for credit reference purposes.

Case 21

The complainant had made a subject access request to an electrical goods company. He did so because he believed the company held inaccurate data referring to his payment record. He received no reply.

The company admitted that the subject access request had not been dealt with. The complainant was sent a copy of the relevant personal data as soon as the error was brought to light.

The company gave assurances that procedures for dealing with subject access requests were to be altered. The complainant's request had been ignored since it was contained within a long letter concerning a different matter. The company's internal guidance notes to staff were being re-drafted to ensure that correspondence would be studied for reference to the Data Protection Act and that consequently access requests would be recognised and acted upon.

Case 22

The complainant was concerned about persistent, unsolicited mailings from an international publishing company, despite his requests for suppression of his details.

It transpired that the complainant's request for suppression had been received by the publishing company, but since it was contained in a reply-paid envelope relating to the subscription offer advertised in the original mailing, this had been immediately sent unopened overseas to the country where membership records were held. The company suppressed the complainant's name and address details and instructed the overseas head office to study all correspondence for such requests and to return any letters which contained such requests immediately.

The company also gave the source of the complainant's address. The list broking company was contacted and confirmed suppression of the complainant's details.

Case 23

The complainant resides in a housing association property where there is accommodation for 103 residents. They do not have individual postal addresses. He applied for credit at a large electrical superstore. His application was rejected and as a result he obtained copies of his credit reference files. Between them they show a variety of adverse information about other residents of the property. The complainant was advised to get a notice of correction put on the credit reference agency's files. This complaint is held pending the resolution of the issue of the use of third party information for credit reference.

Case 24

Almost 200 complaints have been received about canvass forms issued by Community Charge Registration Officers (CCROs) The complaints concerned information collected by CCROs and the manner of its collection. An investigation has been made into the situation in respect of all 403 local authorities. More than 200 "minded to" notices presaging formal action were issued and the bulk of CCROs concerned provided adequate assurances to avoid the necessity for formal action. However, enforcement or refusal of registration notices have been issued against 23 CCROs.

Case 25

The complainant had a mortgage with a large insurance company. His bank statement showed regular payments he could not identify. The bank told him the payments were made to the insurance company and gave him the insurance company's reference. He telephoned the company, gave this reference number and was subsequently given details about another person's insurance cover. He was concerned that he should be given this information over the phone just on the strength of a reference number.

The insurance company stated that there had been an operator error which resulted in the complainant's and the other person's details being amalgamated and the amalgamated record stored. This had resulted in the complainant paying premiums in respect of the other person's insurance whilst his own remained unpaid.

The insurance company would undertake more checks and monitoring to minimise the risk of such errors recurring. Staff dealing with enquiries have been reminded of the importance of the Data Protection Principles.

Case 26

The complainant was told that the local police objected to his application for a licence because he had a previous conviction for attempted murder. He complained that he had never had such a conviction, although he admitted he had had other convictions.

The complainant had been charged with attempted murder but he had been convicted of the lesser charge of assault to cause serious injury. The police records were corrected.

Case 27

The complainant received letters from her building society addressed to her legal personal representatives. She wrote to and telephoned the society to assure them she was alive but kept receiving similarly addressed letters. She complained about the Society's failure to correct its records and the fact that the inaccuracy was adversely affecting her rights as a society member.

The society stated that there was only one file in which the mistake had occurred. The society explained that an indicator had been put against the complainant's name instead of the name following it. The complainant received a full explanation of and an apology for the error.

Case 28

The complainant telephoned an insurance company for a house insurance quote. During the conversation he was asked about convictions. The complainant gave his conviction — 'causing reckless damage to a telephone'. When he received a proposal form his convictions were shown as 'had been convicted of arson or any offence involving dishonesty in respect of property'. Despite several telephone calls, the insurance company did not amend the statement on the proposal forms.

The insurance company had used a standard statement to describe the complainant's conviction which had led to inaccurate data. The insurance company agreed to revise its proposal forms and amend the data relating to the complainant.

Case 29

The complainant kept receiving parcels showing his address which were intended for his neighbour, who had a similar address. The complainant and the neighbour both complained to the mail order company about the inaccurate address but the company ignored these complaints and the parcels were still sent to the complainant's address.

The mail order company stated that it had checked its records and the correct address was recorded on its computer. It had no record of the complainant's address. However, after further investigation the company confirmed that it was holding two addresses for the neighbour. It had amended its records so that the complainant should not receive any further mail or packets for the neighbour.

Case 30

A Citizens Advice Bureau wrote on behalf of a client who cancelled his contract with a rental company. For two months the complainant had received demands for payment of the rent. He was refused credit by another company. On receipt of his credit reference file he found that the inaccurate data had been passed to a credit reference agency. The rental company agreed that due to the delay in the documents reaching its office it had been holding inaccurate data in respect of the complainant. The records were amended and the credit reference agency was advised by the rental company to amend its entry.

A4 Enforcement of the Act

In last year's Report I stated a policy for naming data users involved in prosecution or supervisory action. Broadly speaking, the policy allowed for: giving information about prosecution cases on request, where details were already in the public domain; and publishing information, which can only emanate from this office, in respect of enforcement and other supervisory notices issued. Practice suggests that this policy does not work too fairly for data users, with some names getting publicity and others not. I have held to the policy for this year's Report, but in future years will publish a named list of those involved in prosecution or supervisory action together with the result of that action.

(a) Prosecutions

The Act creates 15 criminal offences and charges have now been brought in respect of 8 of those offences. Charges brought in this year have fallen under the following sections of the Act:

- S5(1) Holding personal data without being registered or without having applied for registration;
- S5(2)(a) Knowingly or recklessly holding personal data not described in the register entry;
- S5(2)(b), (c), (d) Knowingly or recklessly using (b), obtaining (c), or disclosing (d) personal data other than as described in the register entry;
- S6(5) Failure to keep the registered address up to date;
- S6(6) Knowingly or recklessly supplying the Registrar with false or misleading information on an application for registration or for alteration of a register entry;
- S10(9) Failure to comply with an enforcement notice.

During this reporting year I have brought cases against 30 data users. These are listed in the following table. In some cases the data user has been charged with several offences. Twenty-two of those cases have been concluded and a further 8 cases are awaiting hearing. All the cases disposed of to date have been heard by Magistrates Courts but one of the trials pending is to be heard by the Crown Court.

Out of the 25 cases brought against non-registered data users under section 5(1) of the Act, 10 arise out of the failure of the data user to renew his register entry.

Cases Brought in the Year to 31 May 1990

Description of Business of Defendant	Offence (Section of the Act)	Plea	Verdict	Fine £	Costs £
Estate agent	5(1)	Not Guilty	Guilty	500	1,105
Security company	5(1)	Guilty	Guilty	800	100
Employment agency	5(1)	Guilty	Guilty	400	448
Insurance consultants	5(1)	Guilty	Guilty	750	333
Vending company	5(1) 6(5)	Guilty	Guilty	200	
Finance company	5(1) 6(5)	Guilty	Guilty	200	350
Vending company	5(1) 6(5)	Guilty	Guilty	200	
Holding company	5(1) 6(5)	Guilty	Guilty	200	
Engineering Services company	6(5)	Guilty	Guilty	150	50
Insurance broker	5(1)	Guilty	Guilty	150	50
Insurance consultant	5(1)	Guilty	Guilty	500	250
Flying school	5(1)	Guilty	Guilty	400	200
Housing Association	5(1)	Guilty	Guilty	Conditional discharge	
Builders merchants	5(1)	Not Guilty	Guilty	100	300
Theatre trust	5(2)(a) 5(2)(b) 5(2)(c) 5(2)(d)	Not Guilty	Guilty	2,000	900
Company director	6(6)	Guilty	Guilty	1,000	100
Insurance consultant	5(1)	Guilty	Guilty	150	50
Property company	5(1)	Not guilty	Guilty	1,000	600
Medical alarm company	5(1)	Guilty	Guilty	250	150
Computer training company	5(1)	Guilty	Guilty	200	120
Heating equipment company	5(1)	Guilty	Guilty	250	275
Heating equipment company	5(1)	Guilty	Guilty	250	
Stationers	5(1)	Guilty	Not disposed of		
Education foundation	10(9)	Not guilty	Awaiting trial		
Golf Club	5(1)	No plea entered			
Building Society	5(2)(b)	Not guilty	Awaiting trial		
Clothing manufacturer	5(1)	No plea entered			
Mailing organisation	5(1)	Not guilty	Awaiting trial		
Mailing organisation	5(1)	Not guilty	Awaiting trial		
Insurance company	5(1)	No plea entered			

(b) Enforcement Action

During the year 216 preliminary notices have been issued and subsequently there have been 9 enforcement notices and 14 notices of refusal of application for registration. All of these have arisen in connection with the collection and use of information by Community Charge Registration Officers. No de-registration or (overseas) transfer prohibition notices have been issued.

In view both of the number of preliminary notices and the fact that they were resolved by agreement I have not listed the details of them.

Enforcement notices were served on the Community Charge Registration Officers for the following Districts: South Holland; Reigate and Banstead; Thurrock; Great Yarmouth; Dudley; Suffolk Coastal; South Northamptonshire; Wirral; Windsor and Maidenhead.

Notices refusing applications for registration were served on the Community Charge Registration Officers for the following Districts: Castle Point; Llanelli; Cynon Valley; Rhondda; Tandridge; Runnymede; North Bedfordshire; Mid Sussex; Leicester; Chichester; Allerdale; Carrick; Pendle; Melton.

(c) Cases before the Data Protection Tribunal

A data user receiving a notice (enforcement, registration refusal, deregistration or transfer prohibition) may appeal to the Data Protection Tribunal. Three appeals have been made against this year's notices. In addition, one appeal is still pending from a previous enforcement notice. The Data Protection Tribunal has not yet met to consider a case.

(d) The Enforcement Process

It is more efficient to handle prosecution cases at a local level rather than from one United Kingdom office. My Legal Adviser has therefore established a network of solicitors who handle cases in their own areas. The network is not yet complete, but is working well. The solicitors concerned are given training on the Act and the policies and procedures of the office and they, in their turn, provide valuable advice on cases submitted to them.

The Act is a complex piece of legislation and a Magistrates Courts Guidance Pack has been produced with the assistance of Magistrates' Courts organisations, particularly the Justices Clerks' Society. This pack has been distributed to all Magistrates Courts.

A5 The Data Protection Register

This has been a particularly busy year for registration work. Over 100,000 register entries fell due for renewal during the year; there have been more than 19,000 new applications for registration; and over 37,000 amendments to register entries have been received. At the year end there were 153,000 entries on the Register representing about 130,000 data users.

There is no previous experience of registration renewals on which to draw, but the numbers failing to re-register (22%) are higher than anticipated. Now that the peak of renewals has passed, some research will be undertaken to try to determine the precise reasons for this. However, it seems clear that several factors have contributed to this situation — a number of organisations have gone out of business; some larger organisations have reduced their number of register entries; some smaller organisations put in "safety first" applications originally but in practice did not need to register; and others are simply risking being found out.

The registration renewal process is very simple, involving the return of a single sheet of paper. During the year simplified re-registration procedures were introduced for those who just missed a renewal date and again these simply involve the return of a single sheet of paper. There is, therefore, no excuse for those who should have renewed their entry but have failed to do so and, as can be seen from Section A4, the first prosecutions for non-renewal have taken place.

The need to re-register seems to have stimulated a number of amendments to register entries. In the latter part of the year, staff were concentrated on processing applications for registration and work on amendments fell behind by up to three months. This does not cause any legal problem for data users because, once they are received by my Office, amendments are deemed to apply unless and until they are refused. Nevertheless, the backlog is not acceptable as a longer term feature and priority is now being given to dealing with amendments.

The full microfiche version of the Register has been withdrawn from public libraries. It had been placed in 167 public libraries and it was apparent that it was not being widely used. It was also clear that microfiche was not a particularly easy medium for the general public to use. The microfiche has been replaced with an index to the Register, in book form, in 262 libraries. The index refers to a back-up enquiry service from my office. The enquiry service provides any greater detail required on particular entries in the index.

During the year a system has been developed for access to the register using Prestel. The system is now in use in my Office and once it is evaluated, I hope to make it available in selected main public libraries.

A6 Informing People about the Act

This year has seen an innovation in the advertising carried out by the Office. The principal concern since November 1987 has been to ensure that members of the public are aware of the legislation at least in general terms. Allied to this the public need to know who to turn to when they find that something has gone wrong because information about them is kept on computer.

By early 1989 it was becoming clear that the response to national press advertising was falling away. Research also demonstrated that maximum prompted awareness of the legislation had apparently reached a ceiling of about one in three of the population.

Accordingly, in the autumn of 1989 it was decided to mount a television advertising campaign which would target all adults but especially those under fifty-five years of age. Previous research had suggested greater concern about data protection matters amongst those below this age. The objectives would be to raise general awareness of the legislation and also of the Registrar so that people could make use of their legal rights when they needed to.

Television advertising is expensive. With a restricted budget it was essential to produce an economical, but effective, television advertisement which would maximise the funds to be spent on air-time. In the event, it has been possible to run a campaign, consisting of production, air-time and associated research, costing in all about £500,000. The production cost of the advertisement was held to under £80,000. An additional £30,000 was allocated to a telephone response agency to handle requests for the revised rights leaflet which was produced in parallel with the campaign.

The campaign began in February with a test run in the Granada region. The full campaign is based on fairly infrequent selected screenings and I am advised that it is lightweight by industry standards. It has only been possible to construct a realistic campaign by putting money from two budget years back to back across the financial year end. A consequence is that there will be no further funds available for advertising after June 1990 until April 1991.

The information service continues to be heavily used. During the year enquiries staff have handled 41,063 telephone calls, a 29% increase on the previous 12 months. In addition they have responded to 8,607 letters. Since the start of the national television advertising campaign, enquiries from individuals have run at an average of 11% of all telephone calls. This compares with an average of 3% of all telephone calls during the period from June 1989 to January 1990 inclusive.

As in previous years, stands have been taken at a number of exhibitions. Appearances were made at major computer shows in London and Birmingham, and at various more specialised shows in Blackpool, London, Harrogate and Brighton. Over 5,300 visitors collected publications at these exhibitions and more than 1500 specific enquiries were received.

Since the revised (blue) Guidelines were produced in March 1989, approximately 60,000 copies of Guideline 1 and 40,000 copies of each of Guidelines 2-8 have

been distributed. The Guidance Note series has continued to be requested with over 3200 being sent out during the last year.

A new rights leaflet ("If there's a mistake on a computer about you...") was produced to coincide with the launch of the television advertising campaign. In addition to being available through the 0800 television response number and by direct contact with my Office, these leaflets have also been made available through Citizens Advice Bureaux and many libraries.

During the year, staff have given 44 presentations at conferences or seminars, 26 radio and 7 television interviews. The Office has issued 22 news releases and there have been over 1500 press mentions of the Act or the Office.

A7 Background Research

It has been possible to undertake only three pieces of research this year. One of these concerned the question of whether individuals could be uniquely identified from their names and addresses. The brief conclusion from that research is contained in Appendix AA1.

The latest research into public attitudes shows a comparable situation to last year. Public concern about privacy and the holding of information about individuals remains high. Support for the kind of rights given by the Data Protection Act also remains high.

The opportunity was taken during the public attitudes research to assess the early effects of the television advertising campaign (described in Section A6) in raising awareness amongst individuals of both the Act and the Registrar. The programme is not yet completed but, from the research carried out after the test campaign in the Granada region, it seems that the advertisement has impact and is starting to create the increase in awareness intended.

Research results have to be treated with care, for individuals may be informed from other sources than the advertising campaign. However, it seems clear that, following the test run, significantly more people in the Granada region than in the rest of the country were aware: of the consequences of computer error; that they can do something about computer mistakes; and that there is somebody who can help them to get mistakes put right. These were the messages of the advertisement. The full effect of the campaign can only be assessed after an analysis of research to be carried out in mid 1990 when the advertising campaign ceases.

I am also awaiting the results of the latest research into the awareness of the Act and its requirements amongst data users.

A8 International Activities

International interest in data protection is developing rapidly with work taking place in the Council of Europe, the European Community and at the United Nations. Many individual nations are also considering the subject with a view to introducing legislation. Interest is developing not only from matters of internal national policies, but from a renewed consideration of the issue of the transfer of personal data across national boundaries (transborder data flow).

(a) The Council of Europe

My staff have continued to attend as observers at meetings of the Committee of Experts on Data Protection and its working parties. Particular effort has been devoted to the draft recommendations on the protection of personal data used for payment or other related operations. These recommendations will be considered by the Committee of Ministers in September 1990.

Other activities are underway in the Council of Europe in addition to the study of personal identification numbers (PINs) and the working party on information published under statute which are mentioned in Section 2. A study has been completed on the media and the results will be put to the Committee of Ministers. There are also working parties on telecommunications and on medical data.

Ten countries have now ratified the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (European Treaty Series No. 108). They are: Austria, Denmark; France; West Germany; Ireland; Luxembourg; Norway; Spain; Sweden and the United Kingdom. The Netherlands is expected to ratify the Convention this year and Finland is also believed to be close to ratification.

There is an increased interest in data protection in countries in Central and Eastern Europe. It seems likely that any developments in legislation in these countries will be tied in to the Council of Europe Convention.

(b) The European Community (EC)

With the advent of the open market at the end of 1992, the European Commission is giving renewed attention to obtaining equivalent data protection in each of the countries of the Community. The Commission had previously set aside the idea of a directive on data protection and encouraged member nations to sign and ratify the Council of Europe Convention on Data Protection.

From (a) above, it can be seen that eight EC members have, or will soon, ratify the Council of Europe Convention. However, the remaining countries (Italy, Belgium, Greece, Portugal) do not yet have appropriate legislation, although Portugal has relevant constitutional provisions. There is therefore the possibility that there could be a prohibition on the flow of personal data from some members of the EC to others. The Commission has now determined that it will issue a directive on data protection and a draft of this is expected to be published shortly.

Another directive concerning the protection of personal data in the new telecommunications environments, is also anticipated.

The Commission and the Council of Europe jointly hosted a meeting on data protection in Luxembourg in March 1990. This was very well attended by delegates from the United Kingdom.

My Senior Assistant Registrar attended a Commission meeting in Brussels in March 1990 on data protection issues associated with health information.

(c) The United Nations

Data protection is now a topic under consideration at the United Nations.

(d) The International Meeting of Data Commissioners

At its meeting in 1989, the Commissioners passed a resolution on transborder data flows. The resolution is reproduced in Appendix AA3. Broadly speaking the resolution calls for equivalent protection in trading nations as the best way of dealing with transborder data flow problems.

The Commissioners of the EC called attention specifically to the issue in respect of the 1992 open market and the resolution was drawn to the attention of the Presidents of the Council of Ministers, the European Parliament and the European Commission. The EC Data Commissioners also called for data protection safeguards to be applied to Community institutions. They foresaw the need for a data protection authority to cover the work of these institutions, which are not subject to the individual national laws.

A Working Group has been established on Telecommunications and Media under the chairmanship of the Data Protection Commissioner for Berlin. The group has met once during the year to discuss data protection concerns arising from such issues as the use of telephone directory information and caller identification. My Senior Assistant Registrar attended.

(e) Contact with other nations

An Assistant Registrar attended meetings with representatives of other data protection authorities in Copenhagen and Zurich to discuss areas of concern relating to the credit and insurance industries.

There were two meetings of the British and Irish data protection authorities (that is Ireland, Guernsey, Jersey, Isle of Man and the United Kingdom) over the course of the year. These meetings, which were held in the Isle of Man and Dublin, give the opportunity to discuss matters of common interest.

During the year, there have been discussions with my Office by delegations and visitors from Hong Kong, Hungary, Japan, the Netherlands, the Republic of Ireland, New Zealand, Singapore and Sweden.

In April of this year I addressed a conference on data protection in Budapest which was attended by representatives from Eastern European countries. There was considerable interest in the development of this form of legislation. In addition, the Deputy Registrar spoke at a British Council conference in West Germany and my Legal Adviser gave a talk to the International Association of Travel Agents in Portugal about transborder data flow issues.

The year has also seen the introduction of a data protection bill into the United States Congress.

A9 Organisation and Finance

(a) Staffing

Last year I indicated that I would take steps to change the balance of the Office to give more staff in permanent positions and a greater proportion of senior level staff. I have agreed, with the Home Office, changes to staff numbers which allow me to take the first steps in those directions. The Office has been working with about 90 full-time staff, of whom about 30 are employed on a temporary basis. Over the year I have raised the agreed permanent staff levels from 56 to 70 and am now recruiting additional staff at Assistant Registrar and other senior levels for policy and compliance work related to issues such as those in section 2. Further increases in permanent staff are now under consideration.

(b) Staff Representation

I was approached very early on in the life of the Office by one or two trade unions seeking negotiation rights on behalf of staff. I took the view that, providing that more than half the staff were union members and that representation was not through a multiplicity of unions, I was content for staff to determine for themselves how they wished to be represented in general discussions with management. During this year the Civil and Public Services Association (CPSA) and the First Division Association (FDA) recruited more than the required number of staff and a Trade Union Recognition and Procedure Agreement has been reached with them on a joint basis. A joint management/union committee has now been established to take over from the previous management/staff committee.

(c) Finance

Expenditure for the year amounted to £2.98M and there were offsetting receipts of £5.43M. The unaudited financial statements are given in Appendix AA4. The audited account will be certified by the Comptroller and Auditor General and laid before Parliament later this year as required by the Act.

A10 Conclusions

In last year's Report I referred to a consistent and sustained trend towards greater and more complex work loads arising from significant policy issues and from complaints and enforcement activities. That trend has become more pronounced throughout this year.

New senior staff are being recruited to deal with this situation but it will be a few months before they are in post and in the meantime a number of important issues which have been "on hold" must continue in that state. With more staff in post, I hope also to develop a more positive programme of explanation and advice for data users on the requirements of the Data Protection Principles. As can be seen from Section 2(i), a start has been made in the direct marketing sector.

It has continued to be possible to resolve most issues arising under the Act by discussion and agreed action, for example with a data user in the event of a complaint. However, some cases are expected before the Data Protection Tribunal or the courts in the coming year which should lead to a formal determination of some aspects of the current law.

The Interdepartmental Committee chaired by the Home Office has now reported on its review of the Act. Should Ministers and, ultimately, Parliament decide that the Act should be changed, then it appears that new legislation will be required. The various data protection issues now arising may well figure in the debate along with consideration of the interests of the community as a whole, those of computer users and those of individuals. As ever, where potentially clashing public policies occur, the problem will be to achieve the appropriate balances between different public objectives, for example, efficiency and the privacy of individuals.

The widening range of data protection issues seems an inevitable corollary of the increasing development and use of computing and communications technology. The United Kingdom is not unusual in this respect. It is clear that many other countries are now considering these issues and the policy conflicts they may point up. The changes in Eastern Europe and the advent of the open market in the European Community at the end of 1992 are giving added impetus to these considerations.

E. J. Howe
Data Protection Registrar

June 1990

Appendix AA1

The construction and use of Personal Identification Numbers (PINs) — a discussion paper

In order to establish effective relationships between individuals and computer users it is necessary to identify and separate one individual from another. Good identification can have positive benefits both for individuals and computer users. On the other hand, attaching identity labels to individuals can give rise to privacy concerns. For example, common use of such labels can make it easier to collect together and use information about a given individual, even when this is held on disparate computer files by different computer users for unrelated purposes. There are problems associated with this practice of data matching.

More and more information about more and more individuals is being held on computer files and new and improved communications systems make electronic exchanges of information between computer users increasingly possible. In these circumstances, computer users' interest in data matching and in a system of individual identification which would assist this, seems likely to grow. Data protection concerns are likely to grown in tandem. This discussion of individual identification numbers is an introduction to the issues which arise. They are issues of the moment.

Individuals and computer users will wish to establish mutually beneficial relationships. Where these go beyond a simple level (for example a take-away purchase), it will usually be necessary to keep some continuing information on the computer user's files. It will be important, both for an individual and a computer user, that transactions between them can be effectively identified as to whom they relate. Some basic information about the individual will therefore be held to ensure that:

- information is not misattributed from one individual to another;
- advantages due to an individual (eg. goods or services) can be delivered to the correct person;
- things due from an individual (eg. payments or contributions) can be collected by the computer user.

When collecting information from an individual a computer user may seek evidence to confirm that the information given is correct. There are many methods of asking for such confirmation but none of them give the computer user complete certainty. For example, a request to produce a document (driving licence, birth certificate) does not guarantee that the individual presenting it is actually the individual it pertains to.

The computer user may be taking some risk because of this uncertainty, for example when he is providing a statutory benefit or giving value in advance of payment. For this reason he may wish to check with information he already holds to see if he has any record of dealings with this individual. He may also wish to check against information held by others, for example, credit reference agencies. He will need some form of identifying reference in order to locate other relevant transactions with the individual in question.

The information collected and held to identify the individual may vary according to the relationship between the two parties, but might usually include the individual's name and address. This becomes the obvious first possibility for a key to locate and link different transactions with a particular individual. It is valuable, therefore, to consider how far a name and address will uniquely identify an individual.

I have commissioned some research on this and whilst more work needs to be done, the results are of some interest. The research suggests that, distinguishing individuals on the basis of surname, full first forename and address leads to a confusion between different individuals in only 0.9% of cases. In other words, the use of name and address to this level of detail can uniquely identify about 99% of individuals in the United Kingdom population. More sophisticated research, for example examining the effect of using a second initial or full second forename and isolating which particular surnames give rise to most problems, may be helpful. In addition, work may be useful on the effects of mistranscriptions or mis-spellings of names and addresses.

However, once a relationship has been established between an individual and a data user, neither will generally wish to refer to it by a tedious quoting of name and address. Rather, some shorthand reference will be devised and allotted by the computer user. This may be such as a transaction number, a customer number, an account number or a patient number. A convenient generic term for these various references is a Personal Identification Number (PIN). The PINs in use at present are generally specific to a particular computer user and to a particular individual. They are often allotted on a sequential basis and do not generally contain encoded information about the characteristics of the individual.

It is important to have a "second route" to locate transactions about an individual in a computer user's file other than the PIN. This is necessary to cover the situation where the PIN is forgotten or remembered inaccurately. The individual's name and address is likely to provide this route.

It may also be important for a computer user to link relationships with a particular individual which are identified by different PINs. The name and address also offers itself as an identifier for this purpose.

However, a name and address only pertains to a given individual at a given time. Once the individual changes address, that individual in effect assumes another "identity" which is highly likely to be unique to him or her, but is different from the "identity" at the previous address. This gives rise to difficulties in identification where different relationships span changes of address on the part of the individual concerned.

Interest in overcoming uncertainty about the identity of individuals and in permitting identification across disparate relationships leads, from time to time, to demands for the introduction of a national identification scheme. However, as we saw above there is no guarantee, even with such a scheme, that an individual intent on deceit will not simply present false identity documents or numbers. The only sure way of identifying individuals would be through taking details, forcibly if necessary, of some immutable characteristic such as fingerprints or DNA profile. The description of these characteristics would then appear in computer files as the identifier for each set of information held for any given individual.

Moreover, the wide availability and use of a PIN applied to individuals on a national basis (such as the national insurance number) facilitates "data matching". This technique allows the construction of a profile of an individual's life and characteristics from the files of different computer users. There may be occasions where this technique can be used in furthering an important public policy, for example the prevention or detection of crime. These occasions and policies need

to be considered in their own right along with the appropriate safeguards for individuals.

However, data matching as a technique raises data protection concerns. It offers possibilities: for the wide use and disclosure of information without an individual's knowledge or consent; for the use of information out of context to the detriment of individuals; for the wide replication of errors by transferring any inaccurate information from one file to another; for unjust decisions about individuals simply on the basis of a "profile" which causes them to fall into a group with certain selected characteristics; for automatic decision making on facts of doubtful completeness, accuracy or relevance; for the surveillance of individuals; and for influencing peoples lives. There are now specific pieces of legislation or policies to guard against or control this activity in, for example, the United States, Canada and Australia.

It is possible for a de facto common identifier to creep into existence and for this to have national coverage. The wider use of an existing identifier such as the national insurance number is not the only way in which this could occur; the same situation could arise from the encoding of information about individuals into PINs. For example, the use of a combination of name and date of birth to create a PIN, particularly if this were done to a common standard by multiple computer users and applied to a large proportion of the population, might lead to this situation.

It is clearly desirable to seek effective methods which allow computer users to relate information to particular individuals. However, to avoid facilitating indiscriminate data matching, PINs should be specific to the particular computer user or particular context in which the information is held. In addition, such numbers should not contain coded information about individuals.

A Council of Europe working party has carried out a study into the structure and use of personal identification numbers and its report will be placed before the Committee of Ministers in September. The conclusions will provide helpful guidance. However, issues concerned with identifying individuals are already with us, for example, concerned with the linking of information in credit reference agencies' files.

In considering these issues, I should like to see the adoption of PINs which are "context specific" — that is, particular to a given computer user or a given use of personal data. It will help in achieving this if there is a presumption against information about individuals being encoded into PINs held by computer users. If circumstances dictate that it is essential to use such information in that way, then there should be safeguards for individuals. It may be necessary to seek constraints and safeguards not only within the design and operation of the computer system itself, but in agreements, contractual or otherwise, governing the disclosure and use of the PINs and information in question.

E.J. Howe
Data Protection Registrar

June 1990

Appendix AA2

House of Commons Select Committee on Home Affairs enquiry into the National Criminal Records System

A submission by the Data Protection Registrar

1. *Introduction*

This paper considers the National Criminal Records System in the context of the Data Protection Act 1984. The current system, the Act and the advent of the new Police National Computer (PNC2) give rise to a number of questions:

- for what purposes should national criminal records be used?
- what sort of information should the National Criminal Records System contain?
- what type of criminal record should be held?
- how can national criminal records be kept accurate and up to date?
- to whom should national criminal records be disclosed?
- what limitations should be placed on the use of records once disclosed from the national system?
- what safeguards should be established for individuals?
- who should be responsible for establishing, maintaining and controlling a National Criminal Records System?

The paper briefly introduces relevant aspects of the Data Protection Act before considering the questions.

2. *The Data Protection Act 1984*

The Data Protection Act is concerned with information about individuals which is processed by computer (personal data)*. It introduces new rights for individuals to whom that information relates (data subjects). Data subjects may obtain a copy of information held about them on computer (the "subject access" right) and where appropriate have that information corrected or erased. They may also sue for compensation for damage and any associated distress arising from the loss or unauthorised disclosure or destruction of personal data relating to them, or arising from the inaccuracy of such data.

Those who control the contents and use of personal data (data users) are obliged to place details of that use in a public register. They are also required to follow the good practices described in a series of principles (the Data Protection Principles). These Principles are reproduced in Annex 1 (note: in this Annual

*That part of the National Criminal Records System held on microfiche does not fall under the Data Protection Act.

Report the Principles are reproduced in Appendix BB1). The Act allows Orders to be made which would modify the Principles to give additional safeguards in respect of certain kinds of sensitive personal data. These categories of sensitive personal data include criminal convictions. No Orders have yet been made. Nevertheless, such sensitive information demands that the Principles, even as they stand, should be applied with particular care and rigour.

The Act establishes the Data Protection Registrar in a position of independence reporting directly to Parliament. The Registrar is charged with administering the Act and supervising its operation. His decisions are subject to the supervision of the Courts and the Data Protection Tribunal, which is also established by the Act.

The Registrar has a number of statutory duties. These include:

— promoting the observance of the Data Protection Principles;

— considering complaints that the Data Protection Principles or the Act have been contravened and taking appropriate action;

— underpinning compliance with the Act through prosecution for offences or via enforcement action for contraventions of the Data Protection Principles.

The Act recognises the public interest in policing purposes (the prevention or detection of crime and the apprehension or prosecution of offenders). Thus, in any case where these purposes are likely to be prejudiced the police may withhold information from an individual exercising the subject access right; in similar circumstances they are also exempt from the enforcement powers of the Registrar in respect of the "fair obtaining" requirement of the First Data Protection Principle.

The Act is designed to allow the United Kingdom to ratify the Council of Europe "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data". This ratification took place on 1 December 1987.

The Convention has two objectives:

— to protect individuals in circumstances where information about them is processed automatically;

— to facilitate a common international standard of protection for individuals such that the free flow of information across international boundaries can proceed properly.

3. *For what purposes should national criminal records be used?*

The criminal records held on the present system are effectively police records. The contents and use of the records are controlled by the Chief Officers of Police in England, Wales and Scotland. They fall to be data users with attendant obligations under the Data Protection Act. From time to time they will be asked to make the records available for use for other purposes, for example for checking on those who will have responsibilities for caring for children.

The Data Protection Act does not prevent additional uses being made of the criminal records held for policing purposes. The interpretation to the Third Principle effectively allows additional uses as long as they are registered. I am advised that I cannot refuse a registration on the grounds that a use proposed might contravene this Principle, if accepting the registration would cause the Principle to be met.

Certain uses of criminal records other than for policing purposes may be prescribed by statute. Leaving those on one side, extraneous uses of these records seem to be a matter for Chief Officers of Police. It might be argued that this

puts Chief Officers in a difficult position — they are subject to pressure to decide what are effectively matters of broader public interest; and an agreement to further uses of criminal records generates demands on their resources.

Paradoxically, the rights given to individuals under the Data Protection Act have led to criminal records being used for wider purposes. For example, local authorities are requiring individuals applying for a taxi driver's licence to exercise their subject access rights to criminal records and pass on any information received. Some employers are also adopting this technique in respect of potential employees. Whether local authorities and employers should be able to use the National Criminal Records System for their purposes would better be decided on the merits of each case. These extraneous uses should not simply arise through an undesirable manipulation of the Data Protection Act.

Bearing in mind the sensitive nature of criminal records, it would seem appropriate that any uses of them, for other than policing purposes, should be determined as matters of general public interest and policy.

4. *What sort of information should the National Criminal Records System contain?*

A variety of information is currently held in the National Criminal Records System. This includes factual information identifying individuals, the offences for which they have been charged and the results of subsequent cases. It may also include opinion or what might be called "intelligence" information.

It seems clear that the information contained in criminal records has been determined with a view to its relevance for policing purposes. What is not clear is how far all this information is relevant to some of the other uses now made of criminal records. It should be possible, once having determined the uses to be made of criminal records, to determine also the sort of information in the records which is relevant to each defined use.

Such considerations might suggest that the current criminal record files could usefully be treated as separate collections of data; perhaps with factual charge and conviction data being treated differently from other information. This might ensure that information available for non-policing purposes is limited to that which is "adequate, relevant and not excessive" in accordance with the Fourth Data Protection Principle.

5. *What type of criminal record should be held?*

The kinds of criminal record currently held on the National Criminal Records System are restricted to certain categories of reportable offence. The advent of PNC2 will offer the opportunity to collect and process greater volumes of information than at present. As indicated above, the Data Protection Act requires that information shall not be excessive. Care needs to be taken that this new capacity does not simply become a motivating force for extending the scope of the current criminal records.

6. *How can national criminal records be kept accurate and up to date?*

The Fifth Data Protection Principle requires that personal data shall be accurate and where necessary kept up to date. With sensitive data such as criminal records these are clearly important attributes.

The present methods of updating the national criminal records stem from the collection and use of these records by the police. Time has changed both the use of the records and the role of the police in the criminal justice system. It would seem better if responsibilities for updating criminal records were now also changed. It seems probable that records could be kept in the most accurate and up to date condition if those responsible for creating and recording information

within the criminal justice system were also responsible for entering the appropriate information on to the central criminal record. The roles of the police, Crown Prosecution Service and Courts in this process would need clearly defining.

7. *To whom should national criminal records be disclosed?*

Under the Data Protection Act, the power to decide who should have access to the National Criminal Records System (leaving aside any statutory requirements) lies with Chief Officers of Police. Disclosures may be legitimised in the same way as uses (see section 3 above) simply by entering them in the Data Protection Register. I would expect Chief Officers primarily for reasons of policy but also because of pressure on resources, to control such access carefully.

As with the use to be made of criminal records, Chief Officers are placed in a difficult position. At present access may be restricted and kept under the auspices of the Chief Officers. If the advent of PNC2 introduces access points outside the control of Chief Officers then new problems arise. It would be helpful if, as a matter of considered public policy, the persons to whom these records could be disclosed were defined.

8. *What limitations should be placed on the use of criminal records once disclosed from the national system?*

The Data Protection Act would only apply to criminal records, once disclosed, if they were held in a computer system. Even then, as can be seen from the discussion in sections 3 and 7 above, decisions on uses and disclosures would be in the hands of the data user.

It seems appropriate that any public policy determining the conditions under which disclosures may be made from a National Criminal Records System should also set appropriate limitations on the further uses or disclosures of those records.

9. *What safeguards should be established for individuals?*

A number of safeguards have been suggested in previous sections, for example limiting the use and disclosure of criminal records. It is not appropriate to set down an exhaustive set of safeguards here, but some spring readily to mind.

Where criminal records are disclosed then guidelines should be set to restrict their availability to a "strictly need to know" basis. In addition, a concerned individual should also be able to see and challenge the information before any decisions are made on the strength of it. This sort of safeguard is built into the system for the release of criminal records for decisions on those seeking employment in connection with children.

The length of time for which criminal records are to be kept should be carefully set bearing in mind the requirement of the Sixth Data Protection Principle that personal data shall not be kept for any longer than necessary.

Particular attention should be given to the security surrounding criminal records in line with the requirement of the Eighth Data Protection Principle. This will become increasingly important as PNC2 leads to increased networking and a greater number of terminal accesses to the National Criminal Records System.

As criminal records are increasingly held on computer, the subject access right will be available to individuals. Given that criminal records contained only factual information on charges or offences, it would seem questionable whether the subject access exemption, available to the police, should be applied.

10. *Who should be responsible for establishing, maintaining and controlling a National Criminal Records System?*

Use of the National Criminal Records System appears to have developed beyond the stage where it should simply be considered as a police records system.

There seem now to be good arguments for viewing national criminal records in a new light. This would involve determining policies in respect of the nature of information to be held; the use and disclosures to be made of the information; how it is to be collected and maintained; and the safeguards that are to be established for individuals.

Such a review is particularly appropriate at this time when the advent of new technology and techniques makes the accumulation, processing and dissemination of large quantities of data ever more feasible. It is also appropriate in the light of developments of collaborative policing and criminal justice activity within the European Community and on a wider international scale.

In any review of the current system, regard could be had to devolving responsibility to a publicly accountable agency independent of the users of the criminal records. It would be consistent with such an approach that the policies governing the collection and use of criminal records should be clearly visible for public understanding and debate. This should underpin public confidence in a system controlling and processing sensitive information.

E.J. Howe
Data Protection Registrar

21 March 1990

Appendix AA3

Transborder Data Flows — Resolution from the International Data Commissioners' Conference

Each year a meeting is held of Data Protection Commissioners from around the world. In 1989 this meeting was held in Berlin.

The 1989 meeting passed a resolution directed to achieving equivalent protection for personal data in different countries. Such equivalence can give safeguards to individuals and greater certainty to data users in accordance with the general objectives of the Council of Europe Convention on Data Protection.

The growing use of international data networks and the increasing transfer of personal data across national borders gives increasing importance to this issue. The matter attains particular urgency in the European Community because of the advent of the open market at the end of 1992. The detailed resolution follows:

Berlin Resolution of the International Conference of Data Protection Commissioners of 30 August 1989

World-wide telecommunications are evolving rapidly. International data networks are increasingly used for transfers of personal data, for instance in the use of credit cards, for the purposes of travel booking systems and within multinational enterprises. The use of this new technology can bring significant benefits. But it also increases the problem of safeguarding the position of those individuals whose details are transmitted around the world.

The Council of Europe, The OECD, the United Nations and other international organisations have adopted recommendations and guidelines on data protection. A common feature is a set of principles of good practice such as those in the Council of Europe Convention (Treaty 108) and in the OECD guidelines. These good practices are designed to safeguard the privacy of individuals.

So far, eight states have acceded to the Council of Europe Convention and so committed themselves internationally to legally established data protection standards. Data protection authorities in those countries have some authority to control the transborder flow of personal data when this is necessary to protect individuals. However, controlling transborder data flows in this way presents severe practical problems. In most cases, therefore, data transmission across national borders implies that the individual can no longer ensure that the principles laid down by national laws and the various international agreements will be applied to his or her data.

For example there can be no guarantee that the data are up to date, accurate, and used only for proper purposes; and the individual loses the opportunity to appeal to any data protection commissioner.

The solution to giving effective international protection to personal data lies in equivalent legal safeguards in the transmitting and receiving countries. This

solution is consistent with the international recommendations and guidelines referred to above.

The Data Protection Commissioners believe that data protection should be given the same priority as the promotion of data processing and telecommunications in the development and use of international data services. They, therefore, recommend that:

— Governments should move rapidly both individually and through international bodies towards establishing equivalent legal safeguards as soon as possible.

— Those transmitting personal data across national boundaries should check and monitor the protection given to such data by those receiving them, with a view to ensuring that proper regard will be given to the position of individuals.

The objective of these actions should be to ensure that:

— The Basic Principles for Data Protection contained in Treaty 108 and in the OECD guidelines are guaranteed to an individual notwithstanding the transfer of his data across national boundaries;

— Internationally operated data processing systems are structured in such a way that the individual can safeguard his data protection rights without undue difficulty;

— Any correction, up-dating and erasure applied to data which have previously been transmitted abroad will also be applied to the transferred data in any foreign country concerned;

— The greater risks, entailed by international exchanges of data, to the rights of individuals to decide on the use to be made of their data are counterbalanced by international cooperation among data protection commissioners.

Additional statement by the Data Protection Commissioners of the European Community (EC) Nations

The Data Protection Commissioners of the European Community Nations believe that the existence and the activities of the Community give rise both to particular requirements for data protection and to increased opportunities for making data protection effective across national boundaries.

— The EC internal market to be achieved by the end of 1992 is oriented towards the free exchange of information, including personal information, for instance in the fields of direct marketing/address trading and credit reporting.

— European Community decisions increasingly call for the collection and processing of personal data to be carried out by member nations, for instance in the field of agricultural statistics. They also call for transborder data transmission, for instance in the environmental, health-care and social fields.

— Some Community nations are already working on a pilot project to establish common police "wanted persons" files (the Schengen Information System) to provide a substitute, as it were, where controls at internal frontiers are to be abolished.

— On a growing scale, personal information data bases are maintained by the European Community institutions themselves. However, these institutions are not subject to data protection legislation and hence to any requirement to meet the Basic Principles for Data Protection.

The European Community and its member nations are therefore urged to take full account, in their planning for "Europe 1992", of the need for a complete

and consistent approach to implementation of the Basic Principles for Data Protection across community nations and within community activities.

The detailed proposals put forward by the European Community Commissioners are as follows:

— Appropriate legal instruments should ensure that the Basic Principles of Data Protection contained in the Council of Europe Convention (Treaty 108) will be binding on all member nations and on the EC institutions themselves;

— An independent data protection authority should be established to advise the EC institutions on all data protection issues and to supervise the processing of personal data within these institutions. It should consider complaints from individual data subjects and cooperate with the national data protection bodies.

The Commission Nationale de l'Informatique et des Libertes (the French Data Protection Commission) is invited to submit these proposals to the Presidents of the Council of Ministers, of the European Parliament and of the EC Commission as soon as possible and to try to gain their support.

Appendix AA4

Unaudited Financial Statement for the Year ended 31 March 1990

STATEMENT OF RECEIPTS AND PAYMENTS FOR THE PERIOD 1 APRIL 1989 TO 31 MARCH 1990

	Notes	£	1989/90 £	£	1988/89 £
H.M. Grants received	2	2,970,599		2,592,506	
Operating receipts	3	5,264,502	8,235,101	1,206,592	3,799,098
Salaries and Wages		942,777		825,932	
Other operating payments	4	1,945,357	2,888,134	1,758,947	2,584,879
Surplus from operations			5,346,967		1,214,219
Other Receipts	5	163,810		87,664	
Other Payments	5	87,122	76,688	39,618	48,046
Surplus for Year			5,423,655		1,262,265
Appropriations	6		5,400,382		1,353,496
Excess of receipts over payments for the period			23,273		-91,231

STATEMENT OF BALANCES AS AT 31 MARCH 1990

	Notes	1990 £	1989 £
Balance at beginning of period		26,046	117,277
Add excess of receipts over payments for the period		23,273	-91,231
	7	49,319	26,046

The following Notes form part of this Statement

Notes to the Statement

		1989/90 £	1988/89 £
1.	These accounts are drawn up in a form directed by the Secretary of State, and approved by the Treasury.		
2.	HMG Grants Received.		
	Grants received from Class XI Vote 3 Subhead M2 1989-90	2,970,599	2,592,506
3.	Operating Receipts		
	Receipts from registration fees	5,264,502	1,206,592
4.	Other Operating Payments		
	Rents & rates	132,552	128,522
	Maintenance, cleaning, heating & lighting	65,175	61,446
	Office supplies, printing, stationery	49,663	54,663
	Postage & telephones	59,994	39,171
	Travel & subsistence	77,469	70,755
	Staff recruitment	24,493	3,758
	Specialist assistance	17,416	36,788
	Public relations	629,915	756,068
	Legal costs	12,530	11,591
	Staff training/medical	29,400	14,060
	Computer bureau	634,667	395,952
	Vehicle expenses	976	796
	Audit fees	4,600	5,250
	VAT	206,507	180,127
		1,945,357	1,758,947
5.	Other Receipts/Payments		
	Receipts		
	Pension contributions/transfers	17,221	25,763
	Bank interest	111,760	60,608
	Speakers' fees	650	278
	Miscellaneous income	28,983	
	Legal costs recovered	5,196	1,015
		163,810	87,664
	Payments		
	Purchase of computer hardware/software	37,054	11,865
	Purchase of furniture & other office equipment	38,703	22,563
	VAT	11,365	5,190
		87,122	39,618
6.	Appropriations		
	Amounts surrendered to the Consolidated Fund via the Home Office during the period		
	Registration fees	5,236,572	1,262,831
	Other	163,810	90,665
		5,400,382	1,353,496
7.	Balance at Period End		
	Cash at bank	49,053	25,844
	Cash held at offices	266	202
		49,319	26,046

Part B: The Corporate View to 1993

B1 Introduction

The Data Protection Act 1984 is a novel and complex piece of legislation. It deals with a rapidly developing technology which now touches on most aspects of human concern and endeavour. Implementing this legislation calls for consideration not only of the Act itself, but also of other competing public objectives and policies. In these circumstances, it is not easy to get a clear view of the best way to proceed. Nevertheless, it is important to try to map out the road ahead so that efforts can be most purposefully directed towards achieving the Act's goals. This Corporate View does that.

The positive nature of the Act is apparent. There is wide agreement with the new rights the Act confers on individuals. Recent work on reviewing the Act shows strong support amongst data users for the good practices generally stated in the Data Protection Principles.

The Act causes change — improved rights, more open attitudes, sounder practices — change throughout the United Kingdom. It would be foolish to expect such change to be achieved quickly or without cost, or for the achievement to be consistently even in effect across the national community.

The Act breaks new ground. It is also concerned with computing, an all pervasive and rapidly changing technology. In such circumstances the Act may not work precisely as foreseen. As experience is gained of the operation of the Act in practice, this will be reported to Parliament. As part of this process, the Act has recently been reviewed and some modifications have been suggested. It is for Ministers and Parliament to determine if changes should actually be made. If they are made, then, depending on the nature of the changes, this Corporate View may require revision.

This Corporate View covers the three years to the end of March 1993. An introductory background is followed by a statement of corporate objectives and strategies. There is then a list of some significant issues with data protection implications, after which the types of activity to be undertaken are described. The view is completed with an allocation of resources to these activities and a summary of the forecast financial situation.

Whether the Act is changed or not, current experience suggests that events are developing rapidly, such that a view over a period even as short as three years may soon become out of date. This Corporate View will therefore be re-examined from time to time. It is anticipated that the general policies and strategies will hold firm but it may well be necessary to revise the assumed mix and levels of activity and staffing which underpin the financial forecasts. That may in turn cause a review of those forecasts.

B2 Background

2.1 The Data Protection Act 1984

The Data Protection Act received Royal Assent on 12 July 1984. It is the first piece of legislation in the United Kingdom to address the use of computers. It was brought into force in stages. The final stage was in November 1987 when all the new rights for individuals became available and the Registrar's powers came fully into operation.

The Act is designed to allow the united Kingdom to ratify the Council of Europe "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data". This ratification took place on 1 December 1987.

The Convention has two objectives:

— to protect individuals in circumstances where information about them is processed automatically;

— to facilitate a common international standard of protection for individuals such that the free flow of information across international boundaries can proceed properly.

The Data Protection Act is therefore concerned with information about individuals which is processed by computer (personal data). it introduces significant new rights for individuals to whom that information relates (data subjects). Such an individual generally has the right to:

— have a copy of the information about him or her which is held on computers;

— challenge the information if he or she believes it to be wrong and, where appropriate, have it corrected or erased;

— claim compensation for damage and any associated distress arising from the loss or unauthorised destruction or disclosure of personal data relating to him or her, or arising from the inaccuracy of such data.

The Act places obligations on those who use personal data in computers (data users). They must be open about that use (through the Data Protection Register) and follow sound and proper practices (the Data Protection Principles). Computer bureaux have more limited obligations mainly concerned with maintaining appropriate security around personal data. The Data Protection Principles and their interpretations are reproduced in Appendix BB1

The Act establishes the Data Protection Registrar in a position of independence reporting directly to Parliament. The Registrar is charged with administering the Act and supervising its operation. His decisions are subject to the supervision of the Courts and the Data Protection Tribunal, which is also established by the Act.

2.2 The Registrar's Statutory Duties

The Act places a number of statutory duties on the Registrar. Broadly these are to:

- promote the observance of the Data Protection Principles;
- consider complaints that the Data Protection Principles or the Act have been contravened and take appropriate action;
- give information and advice on the operation of the Act;
- encourage the preparation and dissemination of codes of practice for guidance in complying with the Data Protection Principles;
- underpin compliance with the Act through prosecution for offences or via enforcement action for contraventions of the Data Protection Principles;
- compile, maintain and publish a register of data users and computer bureaux.
- give advice and support to other countries which have ratified the Council of Europe Convention.

2.3 The Development of the Registrar's Office

The Registrar took up his post in September 1984. The first permanent offices were opened in March 1985 with a small nucleus of senior staff.

Early effort was inevitably concentrated on the position of data users, particularly with regard to registration. Indeed work on registration has consumed a very significant part of the office's resources and continues to demand a heavy investment.

However, the full introduction of the Act in November 1987 began to change the emphasis. There was a growing need to inform individuals of their rights and a growing number of complaints to consider and determine. The advent of the Registrar's full enforcement powers has also necessitated changes in the approach to achieving compliance with the Act - compliance with the Data Protection Principles has taken its place alongside compliance with registration. Increasingly, there is also a requirement to be involved with, guide and influence policy and practice in issues of wide sectoral or national data protection significance.

It is now about five and a half years since the Registrar entered office. That time has been a period of constant flux for the organisation. This is because of:

- the developing administrative task of establishing an entirely new organisation with its attendant staffing, structure, management and other procedures;
- a constantly changing pattern of work as the Act came progressively into force;
- constantly changing volumes of activity (for example: telephone callers enquiring about the Act were 80,000 in the second year, 17,000 in the third year and 42,000 in the fourth year);
- an increasingly wide and more complex array of issues which have to be resolved as knowledge of the Act spreads and understanding becomes greater.

This developing and changing workload has demanded regular adjustment to the range of skills and numbers of staff required. This problem has been met partially by buying in skills, but primarily by employing temporary staff. This flexible method of staffing has served its purpose well, but it has been causing increasing strains and the Office cannot continue to be run effectively in this way.

2.4 A Complex and Changing Scene

The Office has many communities to serve. They include: the population as a whole; groups representing both data users and individuals; particular data users; particular individuals; and those making public policy. The patterns and volumes of work facing the Office will continue to develop and change. This is inevitable; the Act is part of a rapidly changing and developing social, legal and technological scene.

The latest office research for which results are available shows that public concern about privacy is very high. The evidence collected also suggests that there is continuing anxiety about the amount of information on individuals being kept by organisations. There is continuing and strong support for the right of subject access and the additional rights associated with it.

The legislative climate itself is changing. Already, individuals have been given the right to see manual records held about them relating to social work, housing and, to a limited extent, health. This mirrors concerns on wider issues of freedom of information and either results from or drives the debate on the rights of the individual and the accountability of public authorities or bodies.

There are many new developments in the technology and its use. For example, the development of "smart cards" will bring wider uses of personal data and more people into daily contact with new technology.

In addition to these complexities, the activities and decisions of the Office must have appropriate regard to other public objectives and policies, for example, those concerned with law and order or the welfare of children. Involvement with government departments on developing public policies is an increasing factor in the Office's work.

B3 Corporate Objectives and Strategies

3.1 Introduction

Article 1 of the Council of Europe Convention defines its purpose as "to secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him ("data protection")."

The Explanatory Report accompanying the Convention states that "it is essential....that the undeniable advantages they (data users) can obtain from automatic data processing do not at the same time lead to a weakening of the position of the persons on whom data are stored" ..... "there is a lack of general rules on the storage and use of personal information and in particular, on the question of how individuals can be enabled to exercise control over information relating to themselves which is collected and used by others".

This is the background against which the Act must be seen, but the Act itself does not use these descriptive terms of the Convention. It is described simply as "An Act to regulate the use of automatically processed information relating to individuals and the provision of services in respect of such information."

It can reasonably be argued that the effect of the Act is:

— to create greater openness about the use, through computers, of information about individuals. This being achieved by registration, the subject access right and, in a less direct and positive way, by the requirement that computer users shall obtain information about individuals "fairly";

— to create a situation where information about individuals, which is held on computer, is handled with appropriate care. This being achieved through the acceptance and implementation of practices which meet the Data Protection Principles.

Greater openness facilitates public debate which can guide those considering relevant public policies; the ability for an individual to know of information about him or her facilitates the solution of individual problems. Both openness and good practice in the use of information about individuals should underpin a measure of public confidence which will allow computing to develop and make its beneficial contribution to individuals and the community at large.

3.2 Aims and objectives

Implementing the Data Protection Act can be viewed as a long term major educational programme which is seeking to influence and change the attitudes and practices of a nation. Ultimately the aim is to achieve a situation where:

— data subjects are themselves able to exercise their rights when they wish, both simply and effectively;

— data users, of their own volition, observe the good practices laid down in the Data Protection Principles.

— data protection objectives are considered as a matter of course and given their appropriate weight by those setting public and sectoral policies which involve the use of personal data.

In seeking to achieve this situation, three objectives will be pursued:

— to achieve a public which is informed as to individuals' rights and how to use them;

— to achieve a data user population educated as to the meaning and practical application of the Principles;

— to create an appropriate level of knowledge and understanding of data protection objectives amongst relevant policy makers.

3.2 Strategies

To achieve these aims and objectives, the Registrar will:

(a) Positively inform and guide data subjects and data users on the rights and requirements of the Act.

(b) Underpin the rights given to individuals and resolve the problems of aggrieved individuals, by providing an effective complaints service.

(c) Promote the good practice contained in the Data Protection Principles, by encouraging and supporting the development and adoption of appropriate codes of practice, procedures and techniques by data users and their representative organisations.

(d) Inform and influence those who set public or sectoral policies and practices which might have data protection implications.

(e) Establish openness in the use of personal data by developing and promulgating a Register of data user activities as prescribed by the Act.

(f) Seek to obtain the proper implementation of the Act at minimum complexity and cost to data subjects and data users.

3.3 Supportive Approaches

To support these strategies, the Registrar will:

(a) Resolve particular complaints from individuals and others by:

— seeking a solution through discussion where this achieves a result properly supportive of the Act;

— using the enforcement provisions of the Act where a solution through discussion is not appropriate or attainable.

(b) Obtain compliance by data users with the requirements of the Act through:

— giving guidance as to the meaning of the Act and its application in particular circumstances;

— using the enforcement and offence provisions of the Act where this is appropriate.

(c) Maintain continuing contact with appropriate policy and practice making bodies, in order to be aware of and understand their views and policies.

(d) Develop understanding of and compliance with the Data Protection Principles in selected sectors or for selected computer applications, directing effort towards those activities which seem more sensitive.

(e) Gear up the efforts of the Office by establishing cooperation with representative bodies and by providing supporting effort and material for their own activities.

(f) Maintain a watching brief on matters pertinent to data protection in the United Kingdom, in particular those matters related to the Council of Europe Convention or the European Community.

(g) Monitor the operation of the Act and report to Parliament on this.

(h) Maintain a sound and positive external image of the Registrar's Office and its activities.

B4 Significant Issues

4.1 Introduction

There are an increasing number of developments in both the public and private sector which raise significant data protection issues which will demand action by the Registrar's Office. Some of the developments apparent or foreseen in Spring 1990 are listed here. Experience suggests there is likely to be an increase, both in the number of developments and the complexity of the data protection issues they raise, over the period of the Corporate View.

The list is not in any order of priority. Priorities for action will have to be determined in the light of available resources and:

- the pressure of immediate matters such as complaints from individuals;
- an assessment of the relative sensitivities and importance of different issues at different times;
- the consideration of "windows of opportunity" where it might be possible to exert influence so as to further data protection objectives;
- the feasibility of exerting significant influence on any given issue;
- the pressures of long-term continuing objectives such as public and data user education.

The descriptions of the various developments are very brief and simply give a flavour of the sort of issues which may arise. They are presented under four main headings:

- Applications;
- Legislative and Social Matters;
- Technology and Techniques Developments;
- International Factors.

4.2 Applications.

These include systems for processing personal data which have or seem likely to have significant data protection aspects.

(a) *Computer Developments in the Health Sector*: The proposals in the Government White Papers "Working for Patients" and "Promoting Better Health" will have far reaching implications, including a much greater use of information technology both in the management of the health service and in the provision of clinical care. The question of control over the confidentiality and use of health information is an early issue.

(b) *Police Use of Computers*: Issues will arise from the development of the new Police National Computer System (PNC2). Proposals for a National Criminal Intelligence Unit can also be expected to give rise to data protection considerations.

(c) *Computer Developments within the Inland Revenue*: There are several new developments. They include the BROCS system (Business Review of the Collection System), which is intended to improve coordination of the Revenue's activities and a new database system being developed to build up a detailed picture of the financial activities of suspected tax evaders.

(d) *Computer Developments within the Department of Social Security (DSS)*: The computerisation of DSS offices is an important development which is related to the activities of those who need to liaise with the DSS (for example local authorities administering community charge and housing benefit). Other developments include the introduction of a new system to facilitate the investigation of organised fraud against the DSS.

(e) *The 1991 Population Census*: The Office of Population, Census and Surveys has positively maintained contact with the Office on the potential confidentiality implications of the 1991 Census. Matters under consideration include the security of the Census; the proposal to issue a sample of anonymised records; and the use of small area statistics.

(f) *The Credit Industry*: There is some way to go to resolve the problem of the use of "third party information". Other issues remain, and development work now, for example in connection with the collection and use of comprehensive credit registers, may avoid data protection problems later.

(g) *Direct Marketing*: The collection and use of information about individuals for direct marketing is likely to remain an issue for some time, for example, in respect of lifestyle databases and telephone selling.

(h) *The Insurance Industry*: The industry maintains central registers concerned with life and motor insurance and discussions are underway on the data protection implications of these.

(i) *Telecommunicationx*: The facilities now being developed in support of telecommunications services are leading to the storing of increasing amounts of personal data about telephone calls. Itemised billing and facilities for displaying, on the receiver's telephone, details of the caller's telephone number are the subject of discussions in a Council of Europe Committee.

4.3 Legislative and Social Matters.

These include new public policies and other relevant matters, under debate or foreseen, which will raise data protection issues.

(a) *The Community Charge*: It is likely that issues arising from the collection and use of personal data for the Community Charge will continue for some time.

(b) *The National Football Membership Scheme*: Should this Scheme be reactivated, a number of issues will arise, for example in connection with the "fair obtaining" of information.

(c) *Education*: The changes taking place in the education system will lead to changed and greater uses of personal data in schools and in general education administration.

(d) *The National Criminal Records System*: The recent report from the House of Commons Home Affairs Committee has raised a number of issues with data protection connotations, including the questions of access to be allowed to these records, their accuracy and who should maintain them.

(e) *Identification of Individuals*: The issue of national identity cards and national identity numbers arose during the 1988-89 parliamentary session. Such developments or the development or use of de facto "commonly recognised" identity numbers are likely to be proposed from time to time and will need considering against general data protection objectives.

(f) *Monitoring and Assessment of the Data Protection Act*: A review of the Act was reported to Parliament in mid-1989. An Interdepartmental Committee, under the Chairmanship of the Home Office, is currently reviewing the Act and has recently reported to Ministers. Whatever the results of these two reviews, there will be a need to continue to monitor the working of the legislation. Specific requirements for consultation and for the researching of experience can be expected to arise from time to time.

4.4 Technology and Techniques Developments:

These include technological or systems developments which may affect uses of personal data or may lead to new uses of personal data.

(a) *The Government Data Network*: The Government Data Network is important, not simply in its use by each department, but because it potentially allows the wider use of information across departments. Government departments have made clear that they impose their own strict rules on disclosures of personal data from one to another. A review of these rules with departments could assist public confidence in their operation.

(b) *Smart Cards*: Smart Cards are small, highly transportable computers incorporated in a piece of plastic like a conventional credit card. Smart cards create the potential for individuals to carry collections of personal data with them. This raises a number of questions such as: how the individual can know and check the information held on the card: how access to that information by others can be controlled; whether information available to others from the card is fairly obtained. These are issues which initially might best be examined in the context of specific applications.

(c) *Remote Monitoring Systems*: The development and introduction of systems which can monitor the movements and activities of individuals, pose important questions of data protection and privacy. An example is where a system for giving drivers information on route and traffic conditions, through equipment installed in their vehicles, also records data transmitted back from the vehicle to a control.

(d) *Electronic Funds Transfer at the Point of Sale (EFTPOS)*: The experimental national EFTPOS system has been abandoned and several separate systems are now in place. Data protection issues such as procedures for authenticating individuals and the use of information collected will need consideration.

(e) *Profiling of Individuals*: It is becoming increasingly common to collect more and more details of the characteristics or actions of individuals in order to predict their behaviour. The prediction is based on some level of probability that a certain pattern of behaviour will occur. Inevitably the prediction will be wrong for some individuals who may be disadvantaged by this. Work will be required to see how the technique of profiling and particular applications of it, measure up to data protection requirements.

(f) *Biotechnological Issues (eg. DNA "Fingerprinting")*: There are many areas in which technological innovation is leading to the collection and holding of personal data relating to the biological characteristics of the individual. Some examples are: non-invasive biometric techniques for identifying individuals (automatic recognition of fingerprints, retinal patterns, voice, signature); DNA profiling; genetic screening. All of these require a careful scrutiny from the data protection point of view. Issues such as fair collection, relevance, excessiveness, retention and security come to mind.

(g) *Data Matching*: This technique can be used to draw together information from many different files of personal data. The data within these files will have been collected for many different purposes; the form and content of the data may not be appropriate or directly relevant to the purpose now contemplated; inaccuracies in any file of personal data can be rapidly replicated into other files; and the individual will have no knowledge of these exchanges and uses of personal data about him or herself. The data protection implications of this technique, both in general and in particular applications of it, will require careful assessment.

(h) *Expert Systems*: These systems seek to encapsulate the experience and the decision-making attributes of those skilled in particular disciplines or techniques, for example, the diagnostic knowledge and skills of a doctor. In so far as the automatic decision making of such systems is relied on, then the data on individuals entered into them, and the processing of it, may become particularly critical. Work is needed to examine these developments and understand the data protection implications of particular applications of the technique.

4.5 International Factors

These include activities which it will be important for the United Kingdom to be aware of, learn from or influence.

(a) *Transborder Data Flows*: International communications are developing apace. Transport of data around the world is becoming ever more feasible. The development of "open systems" standards will assist this process. Ensuring that the Council of Europe Convention achieves its objective of protecting personal data properly in these circumstances and that the Data Protection Act plays its proper part in that, demands that attention is given to this topic.

(b) *Recommendations produced by the Council of Europe*: Working parties of the Council of Europe consider problem areas in connection with data protection (for example, concerned with medical data, police data, the identification of individuals) and make appropriate recommendations to member governments. It is necessary to contribute to and learn from this work.

(c) *1992 and the European Community*: The move to the more open European Community raises issues of comparative legislative standards; questions as to transborder data controls; and special matters concerned with cross-border collaboration on the collection and use of personal data, for example, for immigration control and policing.

(d) *International Developments in Data Protection*: It is not only through the Council of Europe that good data protection practice is being developed. The organisation of Economic Cooperation and Development (OECD) has introduced data protection guidelines which are supported by a number of countries. The United Nations is also interested in data protection requirements. It is helpful to remain aware of these initiatives and how data protection practice is developing in countries which follow them.

B5 Activities

5.1 Introduction

Aims, objectives and strategies of themselves achieve nothing. They only become valuable when real work is defined and undertaken. It is appropriate here to consider the kinds of activity necessary to implement the policies already described.

In some cases work will primarily be driven by direct stimuli from outside the Office — complaints and enquiry handling are particular examples of this. Much work arising from the significant issues described in the previous section may fall into this category also. In other cases work will be established as a result of an internal initiative to meet a perceived need or objective — education and awareness work is a key example of this.

However, the activities described do not operate in isolation. They support and are supported by each other. For example: an advertising campaign within the education and awareness activity may be directed to alerting a particular sector as to new guidance in the application of the Data Protection Principles; work on resolving complaints may point to data processing practices with implications beyond the particular data user concerned; enforcement activities may flow from work on promoting the Principles.

Most of the activities are growing in scale and complexity. The activities and some illustrative examples of their scale are:

5.2 Policy and Compliance Work — Promoting observance of the Act and the Data Protection Principles

Work includes: advising data users and assisting them and their representative groups to understand and determine the application of the Act to their interests and activities; encouraging and assisting in the development of codes of practice and techniques to meet the Data Protection Principles; maintaining awareness of new relevant developments in policy, computer applications and technology; ensuring an appropriate data protection input into public policies and new developments at their formative stages; and resolving the application of the Act to major activities such as credit reference or the community charge. Section B4 illustrates the range of issues with which this work will be involved.

5.3 Handling and resolving complaints

This covers: the receipt and consideration of complaints; correspondence with or interviewing of complainants and data users; assessment of the complaint and the data user situation against the requirements of the Act; resolution of the complaint through discussion if possible; and preparation of the case material for enforcement action if appropriate. Volumes of complaints are rising sharply. Almost 2700 complaints were received in the reporting year 1989-90 as against 1122 complaints in the previous year.

5.4 Investigations

This activity: supports the work on complaints; investigates cases of non compliance with the Act, for example a failure to register; contributes case material for enforcement action or prosecutions. The number of assignments undertaken by field investigators has increased by 25% over the two years prior to this review and is forecast to grow to an annual rate of around 1,000 assignments in the first year of the review.

5.5 Registration

This involves: specifying, implementing, reviewing and maintaining systems (manual and computer) and documentation for registration applications, amendments and renewals; resolving enquiries, errors and misunderstandings of data users; notifying data users of register entries, changes and renewal requirements; publishing the register and supplying extracts from it. In total over 190,000 registration applications have been processed and new applications and amendments to the register continue to total over 55,000 per annum.

5.6 The information service

This consists of: a telephone and letter enquiry service for both data users and data subjects; a library; and a service for staff which analyses and reports on external information and provides an information research and monitoring capability on subjects of significant data protection interest. This service has now dealt with over a quarter of a million telephone and letter enquiries. Telephone calls to this service are currently running at 41,000 per annum and letters at almost 9,000 per annum.

5.7 Education and awareness work

This comprises: the development, review and publication of guidelines and guidance notes for data users; the production and distribution of rights leaflets and other information for data subjects, schools, further and higher education establishments and professional adviser services; an exhibitions programme; and media advertising campaigns. This work is fundamental to achieving the knowledgeable public which the Office is seeking to establish. The Guideline Series giving advice on the Act is now in its second edition and over 1.5 million copies of the booklets have been issued. A rights leaflet is also in its second version and around 2 million copies have been issued.

5.8 The legal service

This service: advises the Registrar and other staff on legal aspects of policy and on the application of the Act to specific circumstances; determines the construction and strength of cases for enforcement or prosecution and takes these through the Data Protection Tribunal or the courts. The first enforcement appeal should shortly be heard by the Data Protection Tribunal and other significant enforcement actions are underway. The number of prosecutions is also rising. Some 38 prosecutions have now been undertaken of which 30 were in the last year. In addition, 28 enforcement or registration refusal notices have been issued, 23 of these in the last year.

5.9 Public relations

This comprises: extensive media contact including television and radio interviews; a significant programme of public speaking engagements; and the

preparation and distribution of news releases. This work supports the education and awareness activity, underpins the external image of the Office and directs attention to its role and work. There have now been around 7,000 press mentions of the Act or the Office. Over 200 radio and television interviews have been given and there have been around 400 talks at seminars and conferences.

5.10 Research

This is undertaken in connection with such as: public knowledge of data protection issues and attitudes towards them; experience of data users in implementing the Act and of individuals in using it; the effects of advertising campaigns. The work assists the Office to monitor its progress towards achieving its main aims and objectives.

5.11 International work

This relates to: keeping a watching brief on developments in international treaties and agreements in such as the Council Europe, the OECD, the United Nations and the European Community; understanding developments in data protection practice under other jurisdictions; contributing views on data protection practice flowing from the work of the Registrar's Office, so as to guide and influence appropriate international discussion groups and information exchanges; supporting, on request, data protection authorities in nations which have ratified the council of Europe Convention; establishing and maintaining appropriate international contacts to support this work.

5.12 Corporate services

These cover the normal corporate activities of management, corporate development, finance, personnel, purchasing and office services.

B6 Allocation of Resources

It is planned to allocate resources to the activities described in section B5 in the following way:

	1990-91		1991-92		1992-93	
	Staff %	Total %	Staff %	Total %	Staff %	Total %
Policy and compliance	19 (13)	12 (7)	23	14	23	14
Complaints	13 (13)	6 (6)	14	7	14	7
Investigations	13 (12)	7 (6)	14	7	14	7
Registration	27 (32)	39 (42)	19	33	19	34
Information Services	4 (5)	3 (3)	6	4	6	3
Education and Awareness	2 (2)	14 (19)	2	14	2	14
Legal Services	6 (5)	6 (3)	5	6	5	6
Public Relations	2 (2)	3 (3)	2	3	2	3
Research	– (–)	1 (2)	–	2	–	2
International	1 (1)	1 (1)	1	1	1	1
Corporate Services	13 (15)	8 (8)	14	9	14	9
	100 (100)	100 (100)	100	100	100	100

Notes:
1. The staff percentages are based on a breakdown of salary costs.
2. The total percentages are based on a breakdown of total expenditure.
3. The figures in brackets relate to actual expenditures for 1989–90. They are put in for comparison purposes.

B7 Finance

7.1 Introduction

Section 40(7) of the Data Protection Act states:

> "... the Secretary of State shall have regard to the desirability of securing that those (registration) fees are sufficient to offset the expenses incurred by the Registrar and the Tribunal in discharging their functions under this Act and any expenses of the Secretary of State in respect of the Tribunal."

Financial strategy has been set with a view both to giving proper support for the Registrar to carry out his statutory duties and to achieving this "break even" objective.

The traditional public sector accounting concept of balancing the books in each financial year cannot be applied because of the nature of the registration process. Income from registration fees is received on a cyclical basis determined by the prescribed period of time for which a registration remains valid. This period (set in accordance with Section 8(2) of the Act) is currently three years. Whilst cyclical peaks will gradually be muted, because of a continuing flow of new registrants and a drop out of original registrants, they can be expected to be the significant feature of registration receipts for the foreseeable future.

The Registrar first took up Office in September 1984. The first staff entered employment in the first quarter of 1985 and basic recruitment continued throughout that year. Permanent offices were established in March 1985. Registration commenced in November 1985 and first entries on the Register were made in February 1986. The registration procedures and related computer developments continued throughout 1986. The Act came fully into force in November 1987 and this ushered in a further phase of development connected with the handling of complaints and the use of the Registrar's enforcement powers. The run up to the first renewal procedures in 1989 involved further changes. The Office continues to face new developments as the law is illuminated through case considerations and as technology and the use of computers develop.

In the light of the above, it does not seem unreasonable to treat unrecovered expenditure (£4.54 M) to the end of the 1988-89 financial year (31 March 1989) as concerned with initial set up and development of the organisation. This sum then needs to be recovered over future years. In order to smooth out the future year's patterns of income and registration fees, this recovery is planned over two registration cycles after the first renewal cycle ends in March 1990.

7.2 Financial Forecasts

Year ending 31 March	Office Payments £000	Other Expenditures £000	Receipts £000	Cumulative Financial Position £000
1985	308	22	-	(330)
1986	1,696	50	424	(1,652)
1987	2,422	58	2,757	(1,375)
1988	2,650	60	930	(3,155)
1989	2,624	52	1,294	(4,537)
1990	2,975	70	5,428	(2,154)
1991	3,153	145	2,011	(3,441)
1992	3,742	148	2,960	(4,371)
1993	4,102	152	6,733	(1,892)
Totals	23,672	757	22,537	

Notes:

1. Figures to 1990 are actuals, all other figures are projections. Figures in brackets are negative.

2. Projections include an estimate for inflation. This may, in practice, differ from actual inflation.

3 ."Other expenditures" include estimates of expenditures in respect of the Data Protection Tribunal including those incurred by the Home office.

4. Income figures assume that the Home Secretary raises the fee for a three year registration from £56 (set in January 1989) to £75 in April 1991. Further increases could expect to be needed in April 1993 and April 1995 if break even is to be achieved by 31 March 1996.

5. Proportion of gross expenditure recovered at 31 March 1993 = 92%.

Appendix BB1

The Data Protection Principles

The Data Protection Principles and their interpretations are set out in Schedule 1 of the Data Protection Act 1984 which is reproduced below. Part I of the Schedule states the Principles and Part II gives interpretations to be applied to the Principles.

Schedule 1

The Data Protection Principles

Part I – The Principles

Personal data held by data users

1. The information to be contained in personal data shall be obtained and personal data shall be processed, fairly and lawfully.

2. Personal data shall be held only for one or more specified and lawful purposes.

3. Personal data held for any purpose or purposes shall not be used or disclosed in any manner incompatible with that purpose or those purposes.

4. Personal data held for any purpose or purposes shall be adequate, relevant and not excessive in relation to that purpose or those purposes.

5. Personal data shall be accurate and, where necessary, kept up to date.

6. Personal data held for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

7. An individual shall be entitled-

   (a) at reasonable intervals and without undue delay or expense -

      (i) to be informed by any data user whether he holds personal data of which that individual is the subject; and

      (ii) to access to any such data held by a data user; and

   (b) where appropriate, to have such data corrected or erased.

Personal data held by data users or in respect of which services are provided by persons carrying on computer bureaux

8. Appropriate security measures shall be taken against unauthorised access to, or alteration, disclosure or destruction of, personal data and against accidental loss or destruction of personal data.

Part II – Interpretation
The first principle

1. (1) Subject to sub-paragraph (2) below, in determining whether information was obtained fairly regard shall be had to the method by which it was obtained, including in particular whether any person from whom it was obtained was deceived or misled as to the purpose or purposes for which it is to be held, used or disclosed.

(2) Information shall in any event be treated as obtained fairly if it is obtained from a person who-

(a) is authorised by or under any enactment to supply it; or

(b) is required to supply it by or under any enactment or by any convention or other instrument imposing an international obligation on the United Kingdom;

and in determining whether information was obtained fairly there shall be disregarded any disclosure of the information which is authorised or required by or under any enactment or required by any such convention or other instrument as aforesaid.

The second principle

2. Personal data shall not be treated as held for a specified purpose unless that purpose is described in particulars registered under this Act in relation to the data.

The third principle

3. Personal data shall not be treated as used or disclosed in contravention of this principle unless-

(a) used otherwise than for a purpose of a description registered under this Act in relation to the data; or

(b) disclosed otherwise than to a person of a description so registered.

The fifth principle

4. Any question whether or not personal data are accurate shall be determined as for the purposes of section 22 of this Act* but, in the case of such data as are mentioned in subsection (2) of that section**, this principle shall not be regarded as having been contravened by reason of any inaccuracy in the information there mentioned if the requirements specified in that subsection have been complied with.

The seventh principle

5. (1) Paragraph (a) of this principle shall not be construed as conferring any rights inconsistent with section 21 of this Act.***

(2) In determining whether access to personal data is sought at reasonable intervals regard shall be had to the nature of the data, the purpose for which the data are held and the frequency with which the data are altered.

---

* S22(4) states that data are inaccurate if incorrect or misleading as to any matter of fact.
** S22(2) specifies how a data user may mark information obtained from others so as to safeguard himself against compensation claims in respect of received inaccuracies.
*** S21 specifies the detailed procedures in respect of the "subject access" rights.

(3) The correction or erasure of personal data is appropriate only where necessary for ensuring compliance with the other data protection principles.

The eighth principle

6. Regard shall be had–

(a) to the nature of the personal data and the harm that would result from such access, alteration, disclosure, loss or destruction as are mentioned in this principle; and

(b) to the place where the personal data are stored, to security measures programmed into the relevant equipment and to measures taken for ensuring the reliability of staff having access to the data.

Use for historical, statistical or research purposes

7. Where personal data are held for historical, statistical or research purposes and not used in such a way that damage or distress is, or is likely to be, caused to any data subject-

(a) the information contained in the data shall not be regarded for the purposes of the first principle as obtained unfairly by reason only that its use for any such purpose was not disclosed when it was obtained; and

(b) the data may, notwithstanding the sixth principle, be kept indefinitely.

Printed in the United Kingdom for HMSO
Dd 0504747 C14 7/90 62359 O/N 110908

HMSO publications are available from:

HMSO Publications Centre
(Mail and telephone orders only)
PO Box 276, London SW8 5DT
Telephone orders 071-873 9090
General enquiries 071-873 0011
(queuing system in operation for both numbers)

HMSO Bookshops
49 High Holborn, London WC1V 6HB 071-873 0011 (Counter service only)
258 Broad Street, Birmingham B1 2HE 021-643 3740
Southey House, 33 Wine Street, Bristol BS1 2BQ (0272) 264306
9-21 Princess Street, Manchester M60 8AS 061-834 7201
80 Chichester Street, Belfast BT1 4JY (0232) 238451
71 Lothian Road, Edinburgh EH3 9AZ 031-228 4181

HMSO's Accredited Agents
(see Yellow Pages)

and through good booksellers

ISBN 0 10 247290 4