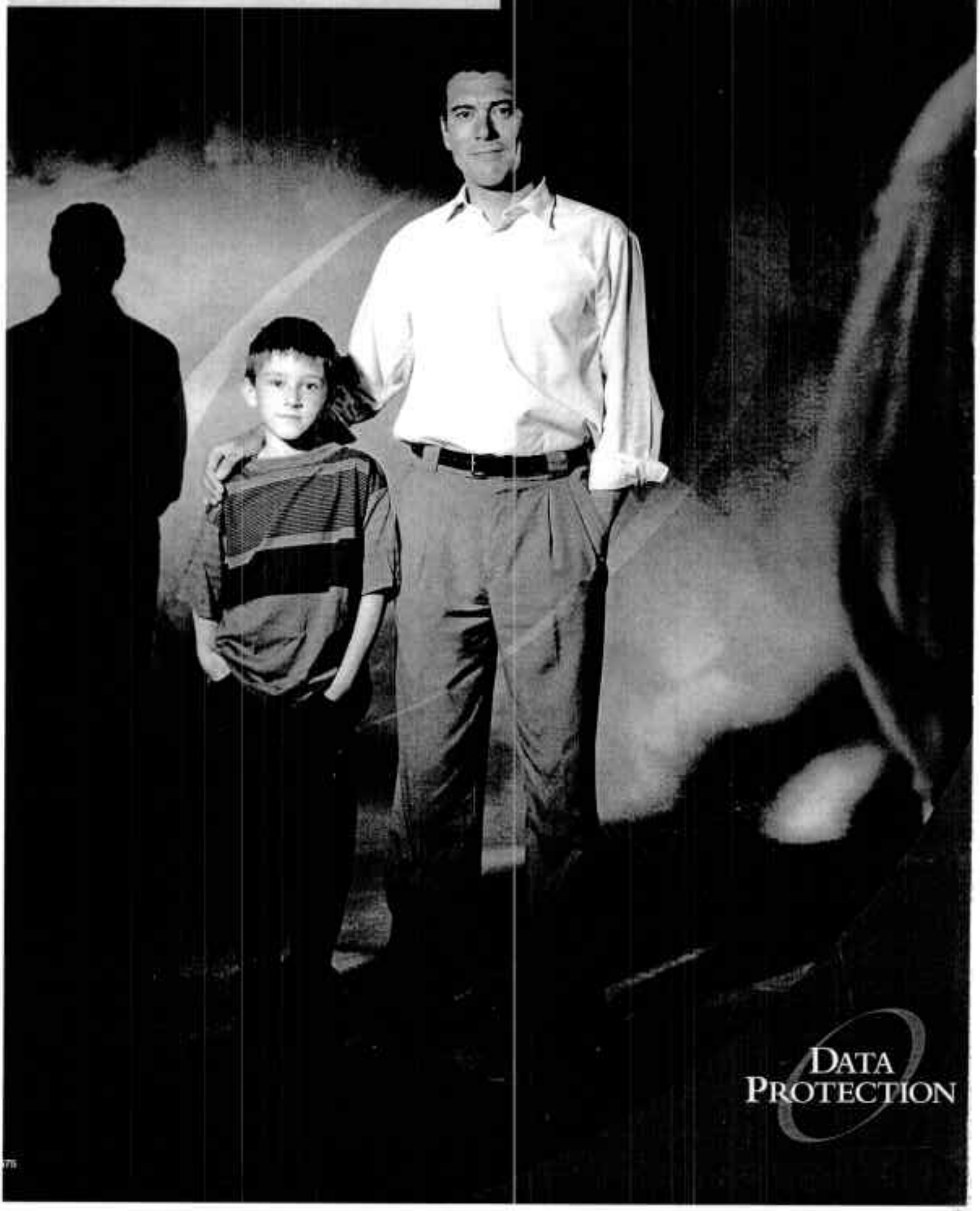
EMBARGO

Not for publication, broadcast or use on club tapes before 12.00 PM on Wednesday July 12th, 2000. This document is issued on the strict understandin that no approach is made to any organisation or person about its contents before that time.

The first report of the Data Protection Commissioner on the 16th year of operation of the Data Protection Act 1984.

June 2000



DATA PROTECTION

our mission

We shall promote **respect** for the private lives of **individuals** and in particular for the privacy of their information by:

implementing the Data Protection Act 1998, and;

influencing national and international thinking on privacy and personal information.

the commissioner's foreword

We have crossed the threshold from theory into practice. On 1 March 2000 the Data Protection Act 1998 came into force. While it was late in the reporting year it was in time for me, as Data Protection Commissioner, to look back on fifteen annual reports of the Registrar's work. Highlights from those reports, charting the progress from Eric Howe's first attempt to predict the impact of the legislation, to this retrospective statement of what happened, form the basis of an annex to this report.

In many ways the 1984 Data Protection Act was ahead of its time, recognising the risk to private life presented by the development of new technology, but uncertain how that risk would manifest itself. Today the part played in our everyday lives by new technology and the processing of personal data which that involves is a significant one. The development of on-line transactions has highlighted some of the risks, but we should not lose sight of the importance of a proper framework of control wherever personal data are processed. What data protection law – new or old – provides is that framework. It is pleasing to report this year the diverse range of data controllers who have recognised this and who have positively embraced the changes which the new law brings. Unfortunately, there remain examples both of those who refuse to see the value or the relevance of the law to their processing – the cry "I only keep names and addresses" can still be heard; and of those who misrepresent its nature. The latter group grasp the Act and wave it as though it were some hybrid garlic which might ward off information hungry vampires. Nowhere does the Act place blanket bars on the disclosure of information. The right to private life, which it seeks to provide the powers to protect, is not dependent wholly, or even mainly, on withholding information. The Act is more complex than that setting out the duties of data controllers and the rights of data subjects and giving equal weight to each of the eight enforceable principles of good information handling:

Data must be:

- fairly and lawfully processed;
- processed for limited purposes;
- adequate, relevant and not excessive;
- accurate;
- not kept longer than necessary;
- processed in accordance with the data subject's rights;
- secure;
- not transferred to countries without adequate protection.

In any event the right is fundamental but not absolute and must be balanced against other rights. For those in the public sector this is perhaps particularly important to keep in mind. Freedom of expression; the aim to have open and accountable public bodies; the public's right to know, have to be balanced against the right to private life. Getting that balance right will be assisted by a statutory framework for access to information. This is a point I made last year in welcoming the proposals for a Freedom of Information Bill. However complex the interface between the two pieces of legislation turns out to be, from my perspective as Data Protection Commissioner the paramount value will be the creation of two sets of statutory rights and obligations.

If the Freedom of Information legislation is enacted as drafted, then the year ahead will be one of more, and in many ways, dramatic change for us. The way that the staff of this Office have responded to the changes we have introduced this year, show that the confidence in them which I expressed last year was well placed. We have moved from handling registrations under the 1984 Act to notifications under the 1998 Act. A doubling of the number of new applications we normally expect to receive in the period either side of 1 March, means that we do have some backlogs. However, the careful preparation and introduction of new procedures, and the willingness of staff across the Office to assist, has kept these at a level we can manage. The move from complaints to assessments has yet to have a measurable impact – the changes there will be for next year's report.

Elizabeth France

Elizabeth France
Data Protection Commissioner

June 2000

review of the year

Last year's annual report set out a list of key objectives for the year. We said we intended to focus on priorities in four areas:

1. Enforcement of the law;
2. The Data Protection Act 1984 (the 1984 Act);
3. The Data Protection Act 1998 (the 1998 Act);
4. The administration of the Office.

ENFORCEMENT - we aimed to:

- oversee, promote and enforce compliance with the Data Protection Act in force, through the provision of ongoing advice, monitoring compliance and taking enforcement action if appropriate.

Although a priority this year has been to prepare for implementation of the 1998 Act, pro-rata we received and handled a record number of complaints, which increased by 36% on the previous year. The number of offences charged under the 1984 Act also increased significantly.

THE 1984 ACT - we aimed to:

- keep up the momentum on our giving of advice and guidance, and on processing new applications for registration and bringing complaints to a satisfactory conclusion;

- reduce work-in-progress to the lowest possible level prior to the implementation of the 1998 Act.

We continued to meet the demand for advice and guidance under the 1984 Act, whilst the number of new applications received and handled increased by nearly 8%. Although we were able to deal with the significantly increased number of complaints during the year, dealing with the unprecedented level of demand at the same time as preparing for and dealing with the new legislation slowed down our closure rates for investigated complaints.

THE 1998 ACT - we aimed to:

- devise a notification scheme to meet the requirements of the Act, and adapt the present registration operating system to run the scheme in the short term;

New procedures have been introduced and the existing system was successfully adapted in time to deal with the required changes. 3,260 notifications were received during March 2000.

- prepare and offer advice and guidance on all aspects of the Act - its requirements, the obligations of data controllers, and the rights of individuals;

- continue to develop and implement training programmes for Office staff, and data controllers;

  We have continued to fulfil demand for guidance on the 1998 Act with 'The Data Protection Act 1998 - An Introduction'. We have also introduced a brief guide to the law for data controllers and a booklet for data subjects on how to use the law to protect their personal information. We have also decided to trial on-line training seminars to make the best use of the Office's resources. These modular seminars will be available to all data controllers towards the end of the year.

- put in place new procedures for handling assessments and prior checking under the new Act;

  Our assessments policy is available on our website. Our procedures for handling assessments were effectively implemented in time for implementation. No categories for prior checking have yet been introduced by the Government.

- carry out a Marketing and Communications campaign to launch the new law, and more importantly, awareness and knowledge of data protection, and compliance with the law.

  On implementation, our new corporate identity was put in place, a press pack was issued to all key journalists and a range of support materials produced for data controllers, including an introductory video on the law. Our broadcast television campaign is planned for August/September 2000.

PROJECTS - we aimed to:

- develop our guidance on the New Act;

  The guidance document 'The Data Protection Act 1998 – An Introduction' has been supplemented by a number of other publications.

- make available guidance on the effect of the new Telecommunications Regulations;

  Interim guidance on the Telecommunications Regulations was issued in June 1999. Further guidance on these Regulations is planned for publication shortly.

- produce a code of practice on the use of CCTV;

  The draft code of practice on CCTV has undergone external validation and is now available on the Commissioner's website.

THE ADMINISTRATION OF THE OFFICE - we aimed to:

- produce accounts on a 'accruals accounting' basis for the financial year 1999/2000;

  We have successfully made the transition from cash accounting to accruals accounting.

- produce longer term proposals to deliver aims set out for bodies such as ours in the "Modernising Government" White Paper.

  Our proposals for meeting these aims were set out in the bid for Capital Modernisation Funds. While that bid was unsuccessful the work done will enable us to bid again for additional funding to make these changes.

central requirements & local issues

Managing the organisation through this year has provided a number of challenges. We are used to change, but the uncertainty over the date of implementation of the 1998 Act and doubts about the volume of work it will generate have involved us in some complex decisions about the use of the resources available to us.

STAFFING MATTERS

Recruitment

A number of problems have become evident during the year.

In the past when we have not been certain of what our longer term requirements might be, we have appointed staff on temporary contracts. The very low unemployment situation in the area - although to be welcomed generally - has made it very difficult to recruit for temporary positions.

All posts have a pay range, and our policy is to appoint at the minimum point in the range. This policy is particularly important in areas where several people do the same job and there would be understandable resentment if those newly appointed are offered more money than those already in post. There is evidence, however, that other local employers - reacting to recruitment difficulties, are much more willing to offer increased salaries to individuals to retain their services. This has led to an increased expectation by those applying for posts that starting pay is a matter for individual negotiation. We have continued to offer starting salaries at the minimum of the range but, given the local situation, we do need to ensure that the rate of progression within ranges is acceptable.

Transfers and secondments

The 'Karolus' Programme which encouraged the exchange of officials within the European Community with the idea of promoting common approaches and standards with regard to community initiatives has been discontinued. Our efforts to send one of our staff on an exchange visit came to nothing but we did host a placement programme for an officer from the Italian Ministry of Defence. Late in the year, we also provided a four week study opportunity for a member of staff from the office of our Hungarian counterparts.

At the very end of the year, we began the process of arranging a six month inward secondment of a solicitor from the Crown Prosecution Service. We are pleased that discussion with the Inland Revenue and DSS has led to an agreement to work together on some of the investigations which impact in their areas. Using their investigative expertise in areas where it is important to them as well as us to see data protection law enforced, gives a welcome boost to the targeted use of resources: a good example of potential 'joined-up' enforcement, on which we hope to report further in future.

Discussions initiated by our counterparts in Australia and Canada to arrange possible job swaps have not been successful to date. However, one of our staff spent two months working for the Organisation for Economic Co-operation and Development in Paris.

There is no doubt that such exchanges offer opportunities to see our work in a wider context and to learn from the experience of others, and we shall continue to pursue and take advantage of any opportunities which we think would be of benefit.

The opportunity to spread Office thinking into other areas is not confined to short term moves. Over the past few years, several staff have moved on into such posts in all sectors of the economy. This year, for example, one member of staff has joined a financial institution to provide compliance advice; another has set up in business as a consultant; and after 12 years as our Legal Adviser, Rosemary Jay has moved into private practice. While we miss the expertise and the comradeship of those who move on, we have always considered that, although it can cause us difficulties in recruiting and training replacements, staff moving on into positions with data protection responsibilities elsewhere is a way of promoting awareness and proper observance of the legislative provisions.

Investors in people

Last year, we reported that we were working towards accreditation as an Investor in People.

Our initial assessment concluded that as the (then) uncertainty with regard to the legislative timetable prevented us from producing an appropriate Business Plan, we ought to consider reapplying once the impacts of the new responsibilities had become clearer and a suitable business plan could be produced.

We have made significant efforts to redress the issues which the lack of planning created and plan to pursue accreditation once the workloads have settled later in the year.

Pay and grading

A number of additional staff have volunteered to become members of the Job Evaluation Panel and have received the appropriate training. We anticipate that office developments are likely to precipitate changes which will require a significant number of re-evaluations, so the increased size of the pool of trained staff will help us to meet that need.

The lack of progression within pay ranges has been a growing issue during the year. In common with a number of other organisations with whom we have regular contact, we have found that the financial constraints within which we have worked since implementing our own pay arrangements have not enabled us to move people within pay ranges as quickly as anticipated. We have had separate discussions with the Trade Union to discuss possible ways of addressing this as part of pay settlements in future years.

Home Office Pay and Superannuation Service (HOPSS) took on responsibility for administering our payroll in June last year. The move was part of the planned move to the Principal Civil Service Pension Scheme (PCSPS) and was an essential forerunner to their taking over the administration of that scheme.

Pensions

Since 1 April last year (1999), all new starters with the Office have become members of the PCSPS. Staff in place on that date had the option of joining the PCSPS and transferring their benefits from the by-analogy scheme. An information pack containing individual benefit statements was circulated to all staff at the beginning of the period during which they had to make a decision on their future pension provider, and experts from both schemes came in to talk to staff about their options. Once the option period came to an end, details were sent to the Government Actuary's Department to enable staff there to calculate a final transfer value.

Staff information

A Management Code was finalised and circulated during the year. The 'Staff Handbook' and 'Health and Safety Manual' were also made available to all staff via the desktop facility on the Office IT network.

Work was begun on a revised and simplified 'Travel and Subsistence Guide'.

PROPERTY MATTERS

Partly with a view to the future possible requirements of the Freedom of Information legislation but also as recognition of the extra responsibilities of the new Data Protection Act, we concluded that we ought to take advantage of a fortuitous development when the only other tenants in the building decided to relocate and offered to discuss our taking over their lease. At year end, negotiations were well advanced to realise that objective. The landlord has also been kept informed as this development means that three separate rental arrangements apply to different parts of the building and, providing an arrangement suitable to both parties can be agreed, it would seem sensible to standardise these.

Negotiations on a possible extension to the lease on the warehouse space in Macclesfield also began towards the end of the year.

FINANCIAL MATTERS

Grant-in-aid

There was only a marginal improvement in terms of the timescale for notification of the level of grant this year compared with last. This late notification reflects the changed timetable which now applies to central budgeting decisions. Recognising that the situation of the last two years is likely to reflect reality henceforth, we have amended the timetable for business planning and related office processes (such as development reviews) accordingly.

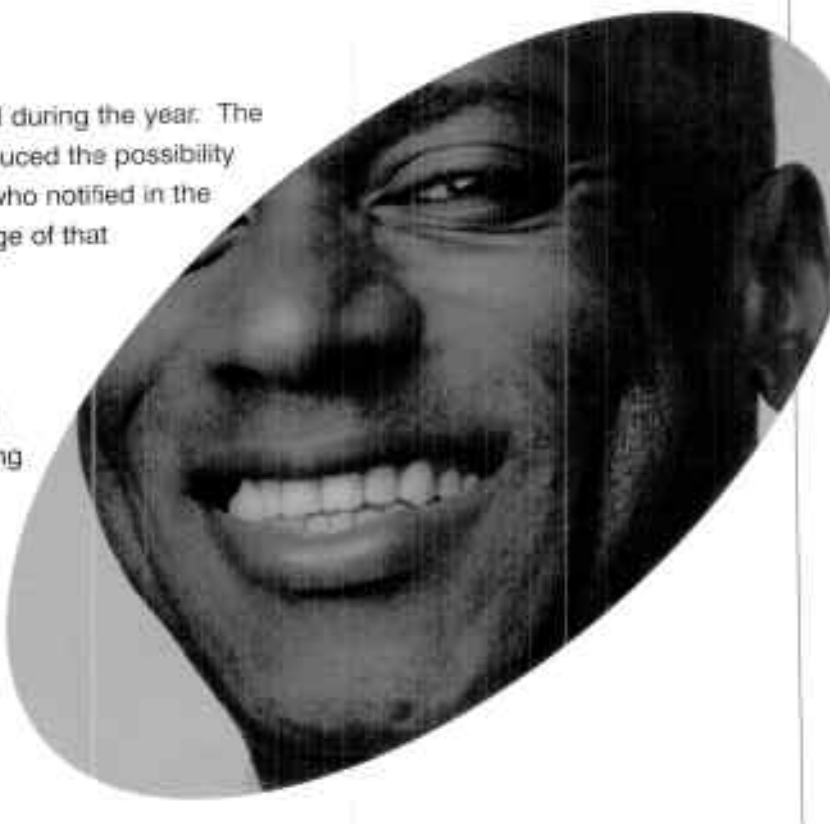
We were pleased that the case which we had made for extra resources to cope with the additional responsibilities received a sympathetic hearing.

Financial regime

The implementation of the new Data Protection Act introduced the possibility of changes to the way in which the Office is funded. We have had some discussions with our sponsor unit and Treasury about the possibilities which these changes introduce. Once we have a clearer picture of the likely effects on revenue of the change in legislative regime, we plan further discussions to determine how best to organise finances in the future.

Income

Fee receipts of almost £5.5 million were received during the year. The change to a single year notification period introduced the possibility of payment by direct debit. Over 25% of those who notified in the early days of the new Act opted to take advantage of that facility.



Internal audit

Home Office Audit and Assurance Unit provided our internal audit function. Their three year rolling programme based on an audit need assessment continued with reports on Budgetary Control, Procurement and Contract Management, Year 2000 Compliance and Key Financial Monitoring.

LONGER TERM PLANNING

Corporate and business planning

The longer term planning process has been complicated by the scale of the possible changes in terms of organisation size and structure which are likely to be necessary as we take on responsibility for Freedom of Information (FOI). We held a number of discussions with a range of organisations to select one to assist us in the process of that change. Workshops involving the whole of the senior management group evaluated organisation and procedural options, and presentations on our early conclusions have been made to all staff. We have been concerned to ensure that any changes made to cope with short term issues fit into the longer term strategy for organisational growth and structure.

Long term investment

We were unsuccessful in our bid for money to improve our IT infrastructure which would have enabled us to make a step change in the way we deliver services. Each year our level of central funding covers our in-year running costs. Even modest levels of investment will equate to large percentage increases on a relatively small budget so, unless a separate funding bid is successful, we find it almost impossible to fund longer term investments.

The work done for the unsuccessful bid will, hopefully, enable us to secure additional funding in the future.

ENVIRONMENTAL MATTERS AND LINKS WITH THE LOCAL COMMUNITY

Environmental actions

A local independent assessment company working in conjunction with the local authority carried out a free review to assess our impact on the local environment and to make recommendations for ways in which we might improve. The report's findings were very positive on the recycling processes which we already have in place, but did identify one potential improvement in the method of disposal of used fluorescent lighting tubes which we have implemented.

Our current building is now almost 10 years old and had begun to show signs of ageing in certain areas. Some maintenance work to preserve the appearance of the outside stonework of the building was carried out during the year.

Archiving and public records

We have continued the project begun last year, confirming the retention periods and procedures for disposal, shredding and recycling of material which is no longer needed.

East Cheshire Hospice

We have continued to contribute to the construction of a Day Care Unit at our local hospice, by encouraging organisations who have benefited from our services to make contributions to the fund. To date approximately £3,640 has been contributed as a result.

Wilmslow High School

We renewed our membership of the local high school picture loan scheme. The pictures by students are displayed in the common areas of the building.

IT MATTERS

During the year a development project was undertaken to adapt our existing registration computer system to handle notifications. An internet system was developed to enable data controllers to complete the notification form on the internet, print it and send it to us.

A project is underway to develop a system to record requests for assessments received under the 1998 Act.

We have been able to introduce some additional internet access points this year and considered the issues of moving on to the Government Secure Intranet (GSI).

Under the terms of our contract with ICL our IT partner, we are in the process of updating all PCs throughout the office and moving to Office 2000 Professional. This will provide us with a much better infrastructure for the coming year.

We have selected a supplier to document image our notification forms and archive them to a CD Rom. This will provide much greater flexibility and ease of access when required.

Year 2000

A Task Force had worked with our IT partners to anticipate problems and to develop contingency measures in the event of any malfunction resulting from the date change. Members of the Team attended the Office on 2 January 2000 to test all systems. The preparations done beforehand ensured that no problems occurred.

OPEN GOVERNMENT

During the year, twelve requests were received under the Code of Practice on Access to Government Information. Ten of the requests were from individuals acting in a personal capacity and two were from journalists. Seven requests were refused. All of those refused were requests for details of investigations into complaints about possible breaches of the Act.

Careful consideration is given to all requests and information is withheld only if one of the exemptions given in the Code applies. In cases where information was withheld, the exemption relating to law enforcement and legal proceedings (Exemption 4) applied.

preparing for implementation

Much of our time this year has been spent ensuring readiness for the new requirements placed upon us by the 1998 Act.

SECONDARY LEGISLATION

One focus of work in the run up to implementation of the Act was the consultation process initiated by the Home Office in relation to the raft of secondary legislation now introduced. We were, as the Act requires, formally consulted on 17 separate pieces of secondary legislation, all of which came into effect on 1 March 2000, the commencement date of the 1998 Act.

Of the secondary legislation introduced under the 1998 Act, the following were subject to the affirmative resolution procedure:

- The Data Protection (Subject Access Modification) (Health) Order 2000;
- The Data Protection (Subject Access Modification) (Education) Order 2000;
- The Data Protection (Subject Access Modification) (Social Work) Order 2000;
- The Data Protection (Processing of Sensitive Personal Data) Order 2000;
- The Data Protection (Designated Codes of Practice) Order 2000;
- The Data Protection (Miscellaneous Subject Access Exemptions) Order 2000;
- The Data Protection (Crown Appointments) Order 2000.

The remaining 10 statutory instruments were subject to the negative resolution procedure. They are as follows:

- The Data Protection (Subject Access) (Fees and Miscellaneous Provisions) Regulations 2000;
- The Data Protection (Notification and Notification Fees) Regulations 2000;
- The Data Protection (Fees under section 19(7)) Regulations 2000;
- The Data Protection (Functions of Designated Authority) Order 2000;

- The Data Protection (International Co-operation) Order 2000;
- The Data Protection (Conditions under Paragraph 3 of Part II of Schedule 1) Order 2000;
- The Data Protection (Corporate Finance Exemption) Order 2000;
- The Data Protection Tribunal (Enforcement Appeals) Rules 2000;
- The Data Protection Tribunal (National Security Appeals) Rules 2000;
- The Consumer Credit (Credit Reference Agency) Regulations 2000.

The consultation process began, on an informal basis, with the submission by the Home Office (and, in the case of one piece of secondary legislation, the Department of Trade and Industry) of the draft statutory instruments proposed. These drafts generated internal discussions and, in a number of cases, discussions and correspondence with the relevant Government Departments before proceeding to the formal stage of consultation. In the case of a number of draft statutory instruments, this consultation process was conducted within tight timescales set by the Home Office.

The extent of the informal consultation and the attention paid to the comments we offered, particularly in the early stages of the process, were welcome.

At the conclusion of the formal consultation process we were able to respond, in each case, indicating that we were content for the statutory instruments to be laid before Parliament. There were some points which remained unresolved but they were not of a significance which would have warranted risking any further delay in the implementation date of the 1998 Act. Experience in practice will indicate whether change is required in these instruments.

One of those about which we had some outstanding concerns is the Data Protection (Processing of Sensitive Personal Data) Order 2000 (the "sensitive data order").

The sensitive data order provides additional conditions relevant for the purposes of the first data protection principle in the case of any processing of sensitive personal data. One of the new requirements of the 1998 Act is that at least one of the conditions (numbering six in all)

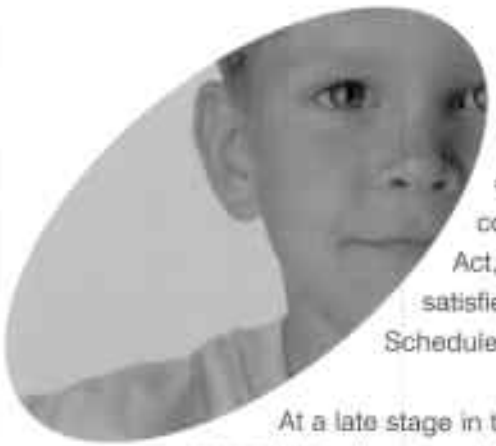
CASE STUDY

Breach of confidentiality by housing association

The complainant had alleged rent arrears with a housing association. She had vacated the property and provided her employer's address for correspondence purposes. The housing association sent a letter to the employer themselves, outlining the amount of alleged debt, and seeking the employer's assurance that they would co-operate should an attachment of earnings order be obtained. A letter addressed to the complainant was enclosed in the same envelope. The complainant claimed she was extremely embarrassed by this disclosure.

The first principle states that data be processed lawfully, which includes common law duties such as the duty of confidentiality. By disclosing this information before obtaining an attachment of earning order, a breach of confidentiality seemed to have occurred, bearing in mind that there would be instances where an order is not granted and the disclosure would be unnecessary.

As a result of this complaint, the housing association undertook in the future not to make such disclosures prior to obtaining an attachment of earnings order.



in Schedule 2 must be satisfied in the case of all processing of personal data. In addition, where there is processing of any sensitive personal data (for example, amongst other things, information about your racial or ethnic origin, political opinions, religious beliefs, or physical or mental health or condition) one of the further conditions provided for in Schedule 3 of the 1998 Act, which includes those contained in the sensitive data order, must also be satisfied. Altogether there are no less than nineteen conditions provided for in Schedule 3 and the sensitive data order.

At a late stage in the consultation process we identified a key area for review. A common example is in the area of holiday bookings made by one person on behalf of a family or group in circumstances where sensitive data may be disclosed, such as the need for wheelchair accommodation or a requirement for kosher meals. The same can also be said in the case of certain insurance arrangements such as health and/or conviction details of proposed named drivers. In many such cases there is some doubt as to whether the explicit consent of the data subject has been obtained.

It has been suggested to us that the law of agency assists in such scenarios, giving the lead member/insured the necessary authority on behalf of the other member(s)/insured (data subjects) to explicitly consent to the processing of sensitive personal data about the data subjects. We accept that on a case-by-case analysis there are likely to be a number of instances where the agency relationship can be established but we do not consider this to be a satisfactory solution to the practical problem facing data controllers in the absence of a condition for processing sensitive personal data which specifically provides for this common circumstance. We would not advise data controllers to rely on the law of agency in all but the clearest cases.

We recognise that it may well be the case that the data subject in question is both fully aware of the need for such information to be provided, and clearly and unambiguously agrees to the lead member/insured providing that information on his or her behalf. However, we take the view that in the majority of cases the consent which the lead member/insured may have, and upon which the data controller relies, is little more than implied or even assumed consent; not explicit consent. In reviewing this aspect of the new legislation and its practical effect we continue to take account of the views of data controllers.

Two statutory instruments were outstanding when the Act came into force, neither critical to its operation during the transitional phase. These are to deal with general identifiers and with processing which requires prior assessment. Amendments have also been found necessary to two others.

ASSESSMENTS

Under the Data Protection Act 1984 there was a duty to consider complaints that raised a matter of substance. Under the Data Protection Act 1998 there is a broad duty to make assessments, on request, as to whether particular processing is likely or unlikely to be compliant with the requirements of the Act.

This change in the scope and emphasis of the duty has also given us the opportunity to reflect on, and learn from, our experience of complaints handling. We have been keen to take that opportunity to do our best to make optimal use of the resources available to us. Exhaustive investigation of the circumstances of particular processing that an individual has raised concerns about, can be very time-consuming. The resources involved can be clearly disproportionate. For example, tracing the source of several mailings to one individual can

involve a great deal of correspondence. Similarly, seeking to resolve a dispute about a minor inaccuracy on an individual's record can take several hours of staff time.

The wide discretion provided by the new law regarding the manner in which an assessment is made gives us the chance to consider how to focus our activity. The resources available will never be enough to investigate thoroughly in every case. Indeed that would not be a proper use of public funds. In many cases a 'summary' assessment, that is one based on the facts as presented by the person making the request together with any information we already have about the processing involved will be sufficient. However, where there is real reason to believe that the processing concerned could have a significant, unwarranted and adverse effect on individuals, an assessment will only be made after an investigation of the facts.

This approach means that some matters which would previously have led to an investigation will now be dealt with on the papers and information available to us. There will be circumstances in which the 'summary' assessment we make will conclude that there is likely to have been a breach of the Act by a data controller. That view will have been formed without our seeking their comments. This will be a change for data controllers, which we shall need to explain to them. It is an approach which will allow us to concentrate on the particular issue of concern to the person who has requested the assessment and will mean the resource we use is proportionate to the likely harm caused by the processing.

The policy we have adopted together with procedures to implement it are available on our website. We shall review them in the light of experience.

NOTIFICATION

A small project team spent this year preparing for the implementation of notification on 1 March 2000. Notification replaces the registration scheme established by the 1984 Act and introduces the most significant amount of change in this area since 1985.

Lengthy discussions took place with the Home Office throughout the year considering the draft notification regulations. Unlike the 1984 Act, much of the detail about notification is contained within this secondary legislation. Of particular interest is the introduction of exemptions from notification for some not for profit organisations and those data controllers who, within certain limits, are only processing personal data for staff administration, accounts and records and to market their own goods and services. Exemption from notification does not, however, mean that data controllers are exempt from the rest of the provisions of the Act.

A great deal of time was spent developing the notification documentation. During February the 'Notification Handbook - A Complete Guide to Notification' was published together with 'Notification Exemptions - A Self Assessment Guide' to enable data controllers to decide for themselves whether notification is required.

A new data controller has a choice in the way in which he can notify. He can call our notification help line and a partially completed notification form based on his nature of business will be sent to him. Alternatively it is possible to complete a notification form on our website, print it and send it to us. This latter system will lay the foundation for a fully electronic notification system once the appropriate infrastructure is in place.

It was not possible, due to financial constraints, to introduce a new computer system to handle notifications. The existing system was successfully adapted to deal with the changes.

Register entries still include a description of the data controller's processing of personal data however, that description is now provided in very general terms. This is a significant change. Other changes include the introduction of an annual renewal and payment by direct debit for the first time, a single notification for each data controller and provision of a security statement. Schools may now notify in the name of the school and partnerships may notify in the name of the partnership.

The implementation of notification went relatively smoothly. There was a tremendous rush to register under the 1984 Act during February 2000 even though there was no significant benefit in doing so and a larger than expected number of data controllers notifying in the first weeks has resulted in higher than expected workloads. This will be addressed in the coming weeks when we will have a much clearer idea of likely volumes.

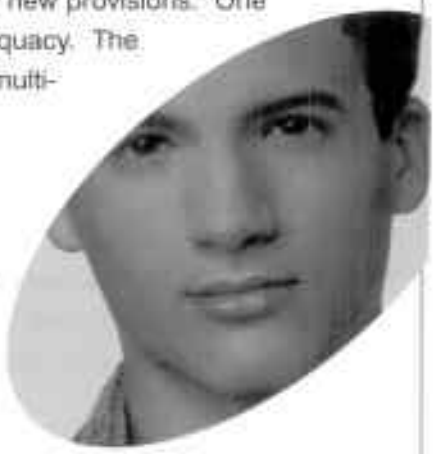
During February the Bar Council advised all barristers that they should notify, and we were inundated with requests to notify from barristers around the implementation date. This surge put our processes under considerable strain at this time.

This coming year will provide our first experience of notification providing us with information about how the exemptions are operating in practice and also information to enable us to develop and enhance our processes. A notification review project is already underway.

TRANSBORDER DATA FLOWS - ADEQUACY OF PROTECTION

In last year's annual report we commented on the provisions of the EU Data Protection Directive, reflected in UK law through Principle 8 of the Data Protection Act 1998, which prohibit personal data transfers to outside the European Union unless there is an adequate level of protection in the overseas country.

In April 1999 we held two workshops attended by industry representatives and lawyers who had expressed a particular interest in trying to resolve the problems posed for businesses by the new provisions. One workshop looked at the use of contractual clauses as a means of ensuring adequacy. The second examined other possibilities such as the use of codes of conduct with multi-national groups.



In the light of comments received at those workshops we issued our 'Legal Analysis and Suggested "Good Practice Approach" to Assessing Adequacy'. In doing so we made clear that these were our preliminary views. We shall be returning to them in the light of developments, some of which are referred to below. To supplement this Legal Analysis we also published practical guidance for data controllers who wish to transfer personal data outside the UK. Copies of both these documents are available under the 'advice and guidance' section of our website.

Meanwhile negotiations continue between the US Department of Commerce and the European Commission on the American proposal to establish a 'safe harbor' for the transfer of personal data to the USA from the EU. The scheme would involve organisations in the States committing themselves to comply with a set of data protection principles backed up by guidance provided through a number of 'frequently asked questions'.

Commitment to 'safe harbors' would provide an adequate level of protection for transfers of personal data to the US from the EU. The negotiations on this issue have been protracted. While a number of EU Commissioners still remain concerned that some of the principles, particularly those dealing with enforcement, need strengthening, the Article 31 Committee representing member states have now accepted the package. We expect the Commission to formally the adopt the proposal this month. It is our view that it is now time to see how the scheme works in practice. If problems do arise, then appropriate remedial action can then be taken. It is clear that the outcome of the 'safe harbor' negotiations is of considerable interest to UK data controllers. We have received a large number of enquiries from companies on this subject, and welcome its imminent resolution.

The EU Data Protection Directive makes provision for the European Commission to find that a third country ensures an adequate level of protection for personal data by reason of its domestic law or of the international commitments it has entered into. The European Commission intend to draw up an 'approved list' of such countries. The opinion of the Article 29 Committee has been sought on the various countries being considered. Switzerland and Hungary are expected to be the first two states to be 'approved' by the Commission.

CASE STUDY

Unlawful procurement

The complainant was subjected to bogus telephone calls, at his home, from someone claiming to be from the Contributions Agency. He reported the matter to the Police who, in turn, notified the Registrar. The Registrar had good reason to suspect information had been unlawfully procured from data users in respect of this complaint and so investigated.

A woman trading as a consultancy from her home address was identified as the operative and she had unlawfully procured information from the Department of Social Security Benefits Agency and from the Inland Revenue.

The woman appeared before Magistrates charged with two offences contrary to section 5(6) of the 1984 Act. She was fined £2,000 on each and ordered to pay costs making a total of nearly £5,000.

Contractual arrangements, which were the subject of one of our workshops, are likely to have an important part to play in securing adequate protection for personal data transferred to outside the EU. We have been involved in the work of a sub-group of the Article 29 Committee considering model clauses submitted to the European Commission by the International Chamber of Commerce. A further model contract, drafted by the UK Confederation of British Industry, is expected to be considered by the Article 29 Committee soon.

SECTION 59 OF THE ACT

Another area where the law requires us to revisit our procedures is section 59, which restricts the information which the Commissioner and our staff can disclose. As a data protection authority, we seek to take the privacy of complainants and others seriously, but we remain of the view that section 59 is overly restrictive. We are keen to demonstrate our commitment to openness as a public body covered by the Open Government Code, particularly in the light of Government proposals on Freedom of Information. However, we are mindful of the importance of clarity for our staff on what should, and should not be provided to enquirers.

With this in mind we have given interim advice to our staff which emphasises the proper balance between the privacy of individuals, the confidentiality of investigations, fair publicity about organisations, and the presumption of openness about information and accountability to the public.

We have concluded that the proper course of action would be to go through a formal public consultation process to determine as far as possible the quantity and quality of information which the Commissioner should publish under her statutory duty in section 51 of the 1998 Act. We have been strengthened in this view by the recent transparency consultation carried out by the Director General of Fair Trading and the emphasis placed on publication schemes in the Freedom of Information Bill. The consultation document has recently been published and is available on our website.

We hope that when we have been able to consider all the responses to the document we shall be able to settle on a policy which addresses most of the doubts about how restrictive section 59 proves to be in practice.

legal developments

In addition to the formal responses to proposals for secondary legislation, set out in Chapter 3, we have been faced with a need for advice on numerous issues, both legal and practical, arising out of the new Act, particularly since implementation. The introductory guide that we published in October 1998 addressed two issues in particular, manual data and the transitional provisions. These were considered to be the most significant issues at the time in terms of preparing for the new regime. Since then we have spent much time considering and advising upon the provisions of the new eighth principle, which is concerned with the transfer of personal data outside the European Economic Area. This advice culminated in a lengthy and detailed paper on the subject which is on our website, also referred to in Chapter 3.

We have produced guidance on the complex issues surrounding subject access and third party information; this is also now on our website. In addition, there was significant legal input to the guidance we produced on the new notification regime, referred to further in Chapter 3.

We are working on a revised edition of the introductory guide to the new Act. This will incorporate references to the subordinate legislation as well as giving further consideration to some of the more pressing issues we have identified. We shall also publish detailed guidance on The Telecommunications (Data Protection and Privacy) Regulations 1999 (the "Telecoms Regulations") to replace the interim guidance published on The Telecommunications (Data Protection and Privacy) (Direct Marketing) Regulations 1998, which came into force on 1 May 1999 and were revoked and superseded by the Telecoms Regulations on 1 March 2000. The Telecoms Regulations fully implement Directive 97/66/EC concerning the processing of personal data and the protection of privacy in the telecommunications sector (the "Telecoms Directive").

Developing the sort of guidance which we produced to assist both individuals and organisations in understanding the 1984 Act is a major exercise. We have set up an internal working group consisting of representatives from across the Office to work over the next year to develop the first edition of "The Guidelines" on the new Act. In the interim, the group will be producing a series of answers to 'frequently asked questions' for publication on our website. We hope that many of the issues that are not covered by our current published guidance will be dealt with, at least initially, in this way.

We produced a booklet, "Private Lives and Judges' Powers" for distribution by the Judicial Studies Board to members of the judiciary, both full and part time. Publication of the planned revised edition to the "Private Lives and Public Powers" booklet has been delayed but it is planned for later this year.

Our legal department worked closely with the Public Record Office in relation to a guide to the new Act for records managers and archivists published on 1 March 2000. This guide was produced by the Public Record Office together with the National Archives of Scotland and the Public Record Office of Northern Ireland and is available from them.

The enforcement caseload has again been varied with a number of cases concerning failed subject access and others involving failed suppression. In those cases in which preliminary notices have been served under our 'fast-track procedure' it has not been necessary to proceed to formal enforcement action. We were satisfied in all such cases that compliance with the data protection principle(s) in question could be achieved without the need for formal enforcement action. In many cases this conclusion has been reached following visits by our compliance staff to the data controllers in question. Such visits have been conducted with the full agreement and co-operation of the data controllers concerned and have proved most helpful and informative.

We have commenced the preliminary stage of enforcement action in relation to contraventions of the Telecommunications Regulations by a number of companies. In light of the high volume of complaints received in this area (see further at Chapter 6) it is likely that the coming year will see further developments in this area.

Work has continued in the utility area. In the last Annual Report of the Registrar we reported on the decision of the Data Protection Tribunal in the appeal brought by Midlands Electricity plc (the "Midlands Electricity case") against an enforcement notice served by the Registrar which restricted the uses which could be made of customer information without the consent of customers. Further to their ruling the Tribunal settled and approved a revised enforcement notice on 20 July 1999, a copy of which is available on our website (the "Midlands notice").

In the last Annual Report we also reported that London Electricity plc and Thames Water Utilities Limited had been served with enforcement notices in the terms of, and at the same time as, the original Midlands Electricity notice and that both companies had also appealed against such notices. Following the issuing of the Midlands notice by the Tribunal, we sought undertakings from both companies in those terms, in the absence of which we would proceed to the Tribunal.

In the case of London Electricity plc, a Tribunal hearing was averted when it was agreed that both the notice and the appeal be withdrawn upon the company giving an undertaking dated 11 January 2000 in terms comparable to the Midlands notice. This undertaking is to come into force on 1 January 2001. A copy of the undertaking is available on our website.

Thames Water Utilities Limited also entered into an undertaking, dated 6 January 2000, again in terms similar to those contained in the Midlands notice but suitably adapted to relate to the provision of water supply, sewerage, drainage and sewage disposal services.

There are three other preliminary enforcement notices outstanding which are being reviewed in light of these developments.

Following the British Gas Trading Limited and the Midlands Electricity plc Tribunal decisions, we have written to all other regional utility supply companies to advise them of the data protection standards with which the Commissioner expects such companies to comply. We shall continue to monitor the compliance of those companies and use enforcement powers, where that seems the most effective way to achieve compliance by all.

The progress of the Freedom of Information Bill, referred to further in Chapter

7, has required careful consideration of the interface between it and the Data Protection Act. It has also provided the opportunity for some valuable amendments to that Act on which we have offered comment.

The Public Interest Disclosure Act 1998 (often referred to as the 'Whistleblowers' Act') came into force on 2 July 1999 and protects workers who make disclosures of information relating to their work from being dismissed or penalised by their employer as a result of the disclosure. The Public Interest Disclosure (Prescribed Persons) Order 1999, which also came into force on 2 July 1999, lists the Commissioner as a *prescribed person* to whom protected disclosures may be made. Disclosures made to the Commissioner are only 'protected' to the extent that they concern the Data Protection Acts 1984 or 1998.

The work on prosecutions has continued to increase. Further warrants have been executed this year in connection with the offences of procuring information contrary to the Act. The facts and figures are set out in Chapter 6.

Our lawyers work on prosecutions with a number of agent solicitors who are based throughout the UK. These solicitors have acquired considerable expertise and knowledge of the 1984 Act. With the introduction of the new Act we held a one day conference in March 2000 to give us the opportunity to discuss the changes which will affect us, particularly with regard to prosecutions under the new Act. All those attending the conference found it a valuable opportunity to talk through the changes and consider ways in which the opportunity might be taken to look again at some of our procedures.

We have taken external advice on the powers of the Audit Commission to conduct the data matching exercises known as the "National Fraud Initiative", referred to further in Chapter 5.

Our lawyers have attended training courses on the Human Rights Act 1998, which comes into force on 2 October 2000. The Legal Department is taking the lead in devising and co-ordinating a rolling programme of training in this area throughout the Office. Such training began during last year with a series of in-house seminars attended by all managers and run by the Legal Adviser. Our investigators have also received initial training from the legal department on the issues arising out of implementation of the Human Rights Act. It is intended in the coming year that human rights training will be rolled out to all staff before October.

the act in action

PUBLIC SECTOR ISSUES

One of the key issues we face in the public sector is the increasing pressure for public bodies to share personal information with other public bodies or to use such information for purposes beyond those for which it was originally obtained. It is encouraging that many bodies now appear aware that there are data protection considerations which need to be addressed in these circumstances and much of our work this year has been devoted to learning about and then advising on a variety of initiatives and working with those involved in an effort to ensure that the appropriate data protection safeguards are put in place before initiatives are implemented.

However, it is not uncommon for us to find that some organisations explain that they will not share information with others on the general grounds that 'the Data Protection Act prevents it' rather than finding out the true position. From our experience such assertions are often used as a convenient catch-all excuse when actually the information sharing cannot take place for other reasons, such as lack of powers or where the data controller is reluctant to share information for other reasons. Many times during the course of the year we have found ourselves advising bodies who have given this blanket assertion, that in fact the Act would permit the disclosure in question or would with a little effort on the part of the data controller. We have even been made aware of cases where the Act is being cited as a reason for not disclosing information where the information requested is not covered by the Act such as aggregated statistical data. Whilst we are pleased that data controllers are mindful of their obligations they must remember that the Act strikes a balance between potentially competing interests and does not represent a comprehensive ban on the sharing of personal information. It is important that Data Protection law is recognised as a safeguard which will give confidence to individuals whose data are obtained by public bodies. It is not helpful if ill-founded citing of the Act leads to it being seen as a barrier to the proper flow of information.

One of the examples of **information sharing** we have looked at is the use of the powers granted to the Department of Social Security (DSS) under section 110 of the Social Security Administration Act 1992. This power gives DSS Inspectors certain powers to require information about employees from employers. The scope of these powers was unclear causing confusion and uncertainty to those organisations approached by the DSS. The DSS are seeking new, more clearly defined legislative powers in the Child Support, Pensions and Social Security Bill. We hope that they will also issue guidance to Inspectors on the use of these powers so as to restrict the likelihood of infringing individuals' privacy.

The Welfare Reform and Pensions Act 1999 provides, amongst other things, for the sharing of certain data between the various bodies who will be involved with the provision and administration of benefits and job seeking activities including the DSS, local authorities, and the private sector. The Act aims to integrate social security and benefits services across government boundaries. This will involve data exchanges between different government bodies, local authorities and private organisations and so clearly raises important privacy

and data protection considerations. It is hoped that such considerations will be addressed both in the legislation and the design of systems and procedures.

Our early involvement where new legislation involves the use and disclosure of information is positive. We consider that our input can only encourage those drafting legislation to be mindful of the privacy rights of those individuals affected by it. We have particular concerns where information collected by one department for one purpose are disclosed to another body for use for another purpose. We believe that to ensure proper scrutiny such provisions should be incorporated on the face of the primary legislation. Where it is determined that they are to be delivered using secondary legislation, we would normally advise affirmative resolution.

As reported in previous years, a number of cases have been brought to our attention where organisations or individuals with no legitimate authority to access data were using a number of means, whether by bribery or deception, to do so. Amendments to the 1984 Act by the Criminal Justice and Public Order Act 1994 made such procuring an offence. An offence of **unlawful obtaining** now exists by virtue of section 55 of the Data Protection Act 1998. There is a move to greater contact with public bodies by remote methods, such as the telephone and increasingly the Internet. If such initiatives are to succeed, it is important to secure the confidence of the citizen in the way their data are handled. We were pleased to discuss with the Inland Revenue the joint use of our resources with a view to tackling the problem of bogus calls made to the Revenue. We hope that our proposed project might go some way to addressing the above concerns and that any lessons we learn might be utilised in future modernising government initiatives.

For some years we have been aware of the practical problems that the Ministry of Defence are faced with in dealing with subject access requests. The many disparate parts of the Ministry of Defence are, in practice, quite autonomous bodies yet, for the purposes of the Act, the department is one data controller. This creates some difficulty in ensuring that an individual has been provided with copies of all the data held about him or her by that

CASE STUDY

Employee sacked for misusing data

The complainant, a student, received a letter from India from someone asking to become her pen-pal. In his letter he said he'd come across her details when developing new software for a company in the UK to which she had applied for a loan. He had noted from the course she was studying that they had similar interests. The complainant was concerned that detailed information she had provided to the loan company in connection with her loan had been used in this way.

The complaint was pursued with the company, raising concerns that live data had apparently been transferred to India for software testing purposes and, that the personal data had been used in this manner by an employee of the company.

It appeared that the loan application forms were passed by the loan company to contractors who sent the information to India, where it was keyed into a database and returned to the loan company by electronic transfer. The employee was not, therefore, a software test engineer but a data input operator. However it was confirmed that all the employees at the site in India had signed confidentiality agreements and as a result of the incident the individual concerned had been sacked.

Solicitors for the loan company contacted the contractors emphasising the gravity of the incident. The contractor responded giving details of various steps that had been taken to prevent a recurrence. These included the placing of notices throughout the keying in facility and weekly meetings, reminding employees of the importance of confidentiality and data protection and the implementation of a targeted 'Employee Data Security Awareness' programme. Also, other employees were informed of the consequences of such a breach and it was cited as an example to future staff. In addition employees were reminded of the effect of such an incident on the contractor's relationship with the loans company and the distress caused to those whose data had been misused.

It was clear from the steps taken by the loan company and the contractor that the incident was taken extremely seriously and that any recurrence of the events which led to the complaint was extremely unlikely.

Department and we have received complaints from individuals about this. Although formal action was considered, the positive response to our concerns and the efforts being put in to address the issue have made this unnecessary.

This year the **Cabinet Office** produced guidance for the Senior Civil Service in relation to the application of the 1998 Act to departments' manual personnel files. Though primarily aimed at the Senior Civil Service, it is hoped that this advice will be promulgated and adhered to throughout the civil service. We welcomed the opportunity to contribute to the discussions that led to the development of this guidance. We were also pleased to speak at the Personnel Director's Group seminar coinciding with the launch of the guidance.

We have welcomed the opportunity to add our comments to the production of the Benefits Agency **'Protection of Customer Information Guide'**. The guide aims to provide advice to DSS employees on when customer information may be disclosed to third parties.

We have continued to have discussions with those Department of Environment, Transport and the Regions (DETR) representatives responsible for taking forward the Government's road user charging proposals. We have raised concerns over clause 171 of the Transport Bill, which sets out information sharing powers to facilitate the road user charging and workplace charging schemes. We are pleased that our concerns about the potential range of purposes to which the information can be put have been addressed with a restriction on use but we remain concerned at the range of bodies who may be required to supply information.

The increasing use of enforcement **cameras on the roads** raises important data protection issues. We are grateful for the opportunity to have discussed these issues with DETR, in particular the appropriate signs we feel should be displayed where such cameras are being used. We also welcome the continuing involvement of the Office in the discussions relating to road user charging as mentioned earlier.

We have been involved in discussions with DETR concerning their proposals to computerise the **MOT system.** Inevitably, contractors are being asked to come up with commercial uses of the information collected for this purpose. We were visited by the project team and provided them with advice on the issues.

This year the Driver and Vehicle Licensing Agency (DVLA) and Driver and Vehicle Licensing Northern Ireland, introduced pilot schemes for **telephone re-licensing.** These schemes permit individuals to renew vehicle excise discs over the phone. Such a scheme will, of course, involve the disclosure of personal data by the driver's insurance company so as to confirm the existence of an appropriate insurance policy. The pilot is to be carried out on the basis of consent.

As reported last year, we have concerns over the purposes for which **access to keeper details** are considered to be "reasonable cause", such as the recovery of civil debts. Following a review, we have been advised that "debt recovery" (including the release of data for council tax purposes) is no longer considered by DETR to amount to "reasonable cause", unless the debt involves some element of the use of the vehicle. We also have concerns about the way in which such disclosures are made, particularly where they are made by electronic links, and the degree to which the DVLA monitors and audits such requests. We continue to have useful discussions with the DVLA on these and other matters and are pleased to note that

the V5 document issued to registered keepers of vehicles has been amended to incorporate a notification of these potential disclosures.

In the last year, we have liaised with the various agencies involved in the multi-agency approach to policing which is advocated by the **Crime and Disorder Act 1998.** This Act allows for partnerships to be formed between local agencies to find solutions to local crime problems. One partnership required by the Act is the **Youth Offending Team,** which comprises representatives from the police, probation, social services, education and health sectors. In order to ensure information sharing is carried out consistently and with regard to the rights of individuals, we have been working with the Youth Justice Board on developing an information sharing protocol, which will set a national standard for Youth Offending Teams. We expect this national standard to provide a model for other types of multi-agency information sharing arrangements, which are being developed as a result of the Crime and Disorder Act 1998.

CASE STUDY

Impersonation

The complainant had three entries on her credit reference file in connection with a CIFAS marker. (Credit Industry Fraud Avoidance System). The markers were put on as a category 3...meaning that the credit application contained material falsehoods. In fact they were in connection with fraudulent applications made by an impostor using the complainants name and address. We approached the lenders and successfully amended the markers to a category 2...impersonation.

We have maintained a productive working relationship with the Association of Chief Police Officers (ACPO) and are pleased that we have been given the opportunity to comment on guidance which ACPO has produced on a number of issues. We were particularly pleased to welcome the ACPO Media Advisory Group guidance on **police disclosure of victim details** to the media, which had been the subject of consultation and concern for some time. We welcome the fact that the victim's consent to such a disclosure will normally be sought, and believe that the guidance strikes the proper balance between the right of individuals to privacy and the right of the media to report on events which may be of interest and concern to the public. The same balance is advocated by the ACPO guidance on disclosure of police video footage to the media.

However, as mentioned at the beginning of this chapter, there are instances where data controllers, for a variety of reasons, decide not to disclose personal information even though the Act would not restrict disclosure. Although the ACPO media guidelines provide sensible practical guidance on what may be disclosed to the media, representatives of the media are expressing concern that the guidance is not being applied correctly or consistently by police forces around the country. This is a matter of concern to us. We do not wish to see what are often viewed as arbitrary restrictions on disclosure imposed where there is a quite proper basis in law for the disclosure to take place. During the year we shall continue to work with the police and media to ensure that the guidelines are fully understood and encourage their consistent application by all police forces.

We are currently consulting with **ACPO Data Protection Working Group** on a revised code of practice on data protection. The implementation of the new Act has provided the opportunity to revisit the current code of practice and update it both in light of developments in data protection legislation, and changes in policing practice.

The experience from this exercise will inform discussions that we are also having with the **Association of Chief Officers of Probation** on a similar code of practice on data protection.

The **National Health Service's** techniques for delivering healthcare to patients have continued to develop rapidly and we have continued to monitor those developments. The implementation of services such as NHS Direct, the establishment of new electronic databases and the use of telemedicine will oblige the NHS to face many of the issues that have already been faced by other sectors - for example how to establish a reliable means for verifying the identity of telephone callers.

Electronic records relating to patients are being developed, as are the new administrative databases needed to support those records. The NHS Strategic Tracing Service, for example, will allow an individual's unique NHS number to be derived from his name and address. This will allow healthcare staff to enjoy easier and more reliable access to the information that they need to treat patients.

Whilst there can be little doubt as to the benefits to patients that the new techniques for healthcare delivery will bring, the development of those techniques, and in particular the processing of personal data needed to support them, raise concerns about personal privacy. Those concerns are accentuated when the proportion of the population whose data will be processed is appreciated. We have, therefore, been in close consultation with the Department of Health. Our aim is to ensure that the evolution of the NHS's techniques for delivering healthcare to individuals does not lead to any erosion of the right to medical confidentiality that individuals have traditionally enjoyed. We are therefore keen to encourage the Department of Health, the medical research community and others to initiate a programme of public education. Part of the solution lies in making individuals aware of how information about them will be processed, and to ensure that they can readily exercise their rights. We welcome the establishment of the **National Confidentiality and Security Advisory body.** This is being set up to advise on the ethical, practical, technical and managerial aspects of confidentiality and information security and we hope to be involved in its work. It is also encouraging that **Caldicott Committee's recommendations** for reviewing the use of patient identifiable information in the NHS are continuing to be implemented.

The move towards 'joined up' or 'seamless' **inter-agency care** continues. We recognise the benefits to individuals this can bring but vigilance is needed to ensure that the approach addresses concerns about personal privacy, as well as the wider questions about the basis on which individuals use the NHS or social services. It is not always clear when and to what extent individuals have a choice as to how the information that they provide to their doctor or social worker will be processed.

Included as an appendix to last year's annual report was our response to the **Modernising Government** White Paper. We welcomed the acknowledgement given in the paper that data protection should be viewed both as an as an end it itself ("an objective of information age government rather than an obstacle to it") and as a means of building public support for the modernising government agenda. The paper made a number of specific commitments on privacy:

- to work closely with the Data Protection Commissioner;
- to carry through our commitment to openness;

- to take advantage of the Commissioner's powers to conduct assessments of the processing of personal data;
- to promote specific codes of practice;
- to deploy privacy enhancing technologies;
- to provide a proper and lawful basis for information sharing.

In a number of areas it is too early to comment upon the extent to which the Government has delivered on these commitments. As we report elsewhere, for instance, work on developing an audit methodology, which will be the basis of the good practice assessments conducted by the Commissioner, is only just reaching completion. Nevertheless, a year on, it is useful to take stock of progress.

In a number of areas we can record an increased willingness by central government departments, agencies and local government to seek advice from our Office and to shape initiatives and policy proposals in the light of the advice given. For instance, we welcome the opportunity to have input into the authentication and smart card frameworks developed by the Central Computer and Telecommunications Agency and Central IT Unit (CITU). We have also had useful exchanges with many other bodies over issues arising out of the joined-up government project, including the Office of National Statistics, the Benefits Fraud Inspectorate and with the public audit bodies through the **Public Audit Forum** over data sharing and data matching issues and with bodies representing trading standards officers and fire brigades of the developments of sectoral codes of practice.

CASE STUDY

Council makes unlawful disclosure of personal data

The complainant was in receipt of income support, incapacity benefit and housing benefit. He had made arrangements for his housing benefit to be paid direct to his landlord, as rent.

As a result of a change in his circumstances his income support stopped, although at the same time his incapacity benefit increased. He complained to the Registrar that when this happened his local council's housing benefit department disclosed to his landlord's agent details of the resulting changes in his housing benefit, and demanded repayment of overpaid rent from the landlord, rather than from himself.

Although housing benefit regulations allow payments of housing benefit to be made to landlords, and impose a duty on landlords to notify local authorities of any circumstances which might affect the claimant's entitlement to housing benefit, we did not know whether those regulations allow disclosures such as had occurred in this case. If not it is likely that the council had processed the data unlawfully and thus outside the terms of the first Data Protection Principle.

The complaint was pursued with the council who confirmed that the disclosure should not have been made. Although the relevant regulations allow a local authority to recover overpayments from a landlord or a tenant, in this case they were wrongly interpreted by a member of staff who sent a notification of recoverable overpayment to the landlord's agent rather than the tenant. The Council accepted that this should not have occurred and as a result of the error circulated a memo to all staff reminding them that landlords must not be sent overpayment letters unless the landlord is responsible for the repayment.

As central and local government become more comfortable with the idea of seeking data protection advice in the planning stage of projects, there are resource implications for us which must be addressed if advice is to be given in a timely and effective manner. For instance, while we were pleased to have the opportunity to comment on drafts of reports prepared by a number of the Policy Action Teams (PATs) established by the Social Exclusion Unit, it was frustrating to have to repeat the same points to each of the PATs rather than to have a single point of contact.

As an initial step more contact with the Information Age Champions Group, which meets under the auspices of the Central IT Unit, would be helpful.

This problem can be particularly acute in the local government area where it can sometimes seem as if all 450 UK local authorities are independently seeking the same advice. In this context we are pleased to report that some progress has been made over the past twelve months in implementing a more comprehensive approach to the local government sector. In June we invited a representative group of local authority data protection officers to a meeting at our offices to discuss the way forward. The meeting was able to agree a number of proposals for the development of sector wide advice and guidance and for the provision of training to data protection officers. In recent weeks we have also had some helpful discussions with representatives of the **Local Government Association** as to how to incorporate data protection considerations in the various information age government initiatives with which it is involved.

In addition to organisational solutions to the problem of how to respond effectively to increased requests for advice, we have argued for the development of a government wide privacy policy building upon the commitments given in the White Paper. Among the purposes of such a policy would be to ensure a more consistent approach to data protection and privacy questions across central and local government and to raise the base level of data protection knowledge thus allowing us to focus upon new questions. In this context we welcome the indications we have received from CITU that they propose to develop such a policy by March 2001.

The 1998 Act lays considerable emphasis on the development of Codes of Practice whether by the Commissioner or by data controllers designed to foster good practice. Even though the Act has only been implemented since March, it is encouraging to report that we have had some discussions with the Office of National Statistics (ONS) on the development of a **government-wide code of practice on the sharing of information for statistical purposes.** We are particularly pleased to report that in addition to beginning work on the revision of its own code of practice on data matching, the DSS has contacted the Local Government Association, DETR and a number of other central government departments with a view to developing some high level **guidance on data matching.**

In reporting on these developments, we emphasise our experience of the effectiveness of codes of practice both in ensuring compliance with the Act and in building public confidence in information handling practices. In the controversial area of data matching, for instance, it is notable that where effective codes of practice are in place, we have received relatively few complaints. This is true of data matching carried out at a national level by the DSS, and at a local level, for instance by a number of local authorities in Scotland.

In previous years (e.g. Appendix 11, 13th Annual Report) we have advocated the adoption of a design philosophy whose aim is to deliver privacy to the citizen. The support for this concept in the Modernising Government White Paper was therefore welcome. That the deployment of such a design philosophy has been slow is perhaps not surprising, given that some of the technologies that might be employed are in their infancy and given that the concept is in some ways contra-intuitive.

CASE STUDY

Unsolicited mailings

A husband and wife received unsolicited marketing literature from a bank. Despite writing to the bank on at least six occasions to request that no further mailings be sent, the bank failed to comply with the request and continued to send literature. A complaint was made to the Data Protection Registrar which resulted in the bank amending its database to ensure that no further mailings were sent to this address.

It is therefore pleasing to report on the conclusion of a long discussion with the Department for Education and Employment regarding the allocation of **unique reference numbers to school pupils** (see 14th Annual Report). The Department wished to allocate numbers to school pupils for two principal reasons: to facilitate the production of more reliable statistics through being able to link the records of pupils held by different schools which they may have attended during their academic careers, and occasionally to allow the Department to furnish a school with a basic academic record (which the department will hold for statistical purposes) in cases where the full record has not been supplied by a school previously attended. Our criticism of the original proposal was that placing a unique number on all pupil records and permitting the use of that number in a large number of different contexts would allow the unauthorised matching of data or the tracing of vulnerable pupils or their parents through the education system. The solution finally adopted involves the allocation of a unique number by the school first attended by a pupil but restricts the use of that number so that it is in effect an internal reference number rather than one by which pupils or their parent identify themselves. The number will only be disclosed to a new school attended by the pupil or to the DfEE for use in compiling statistics. Once the number is transferred to the DfEE it will be translated in a secure, encrypted fashion into a national number. Although this can be decrypted when the Department needs to communicate a record to a school, its only routine use will be in linking records for statistical purposes. Since the national number will never be known to anyone outside the Department, it cannot be used to trace individual pupils. We very much hope that this will be the first of many examples of the use of **privacy enhancing technologies.**

Another example is the Department of Social Security who will be replacing their computer systems over the next decade. We have welcomed the opportunity to meet with those involved in the design of the new systems. This has given us the opportunity to explain some of the difficulties that have arisen in the past as a result of poor system design with a view to eradicating such problems in the future.

In last year's report we commented upon the **National Fraud Initiative** (NFI) conducted under the auspices of the Audit Commission. This exercise involves the electronic comparison of sets of data held for various purposes, notably, personnel, benefits and licensing purposes by local authorities in order to identify possible cases of fraud. For instance, the comparison of records held by two neighbouring authorities may suggest that the same individual is fraudulently in receipt of a student award from one and housing benefit from the other. Our concerns are that because bodies subject to audit by the Commission are under a duty to provide sets of data that the fair obtaining provisions of the Act are effectively disapplied. We also have concerns that the exercise could develop beyond the identification of fraud into areas such as debt tracing.

As this issue is still under discussion with the Audit Commission, it is not appropriate therefore to comment in detail. It is, however, worth reporting upon the advice which we have obtained from leading counsel. In brief this suggests that the NFI may well contravene the Human Rights Act (with effect from 2 October 2000) because of the lack of safeguards for individuals. Our discussions with the Audit Commission are

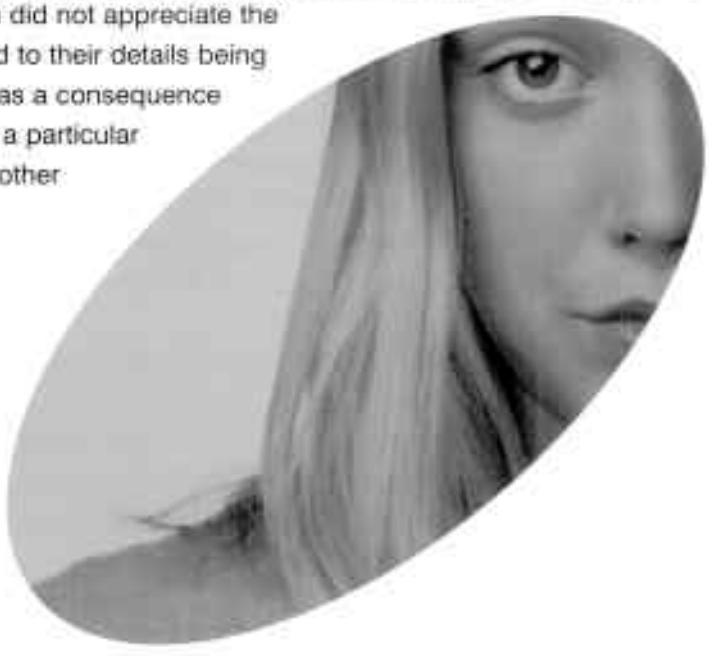
designed to find ways in which the NFI might be conducted upon a clearer basis, confined to the area of fraud prevention and carried out within the framework of rights established by the Data Protection Act. The case is significant in our view, partly because of the very large number of people affected, but also because it throws into sharp focus the nature of the commitment given in the White Paper to ensure a lawful basis for information exchange.

THE USE OF MEMBERSHIP DETAILS

During the past two years we have received a number of complaints regarding the use of membership lists of political parties. Most recently there was considerable publicity concerning the use of the Labour Party list of London members by those promoting Frank Dobson in his campaign to be the official Labour Party candidate for the London Mayoral election. We carried out an investigation into the circumstances surrounding this mailing. It was clear from that investigation that some significant data problems can arise when a membership list is traditionally made available to those such as Branch and Constituency Secretaries, MPs and MEPs. In such circumstances there is a very real prospect of the data concerned finding its way into the hands of a group within the party seeking to promote a particular candidate or candidates in internal elections.

A copy of the press release issued is available on our website.

This highlights a need for all membership organisations, including Trade Unions and charities to ensure that, at the outset, it is made absolutely clear to those wishing to take out, or renew, membership how widely their details will be made available and for what purposes. Where membership information is going to be widely distributed so that there is a likelihood of it finding its way into the hands of a particular group of members keen to promote the views of a sectional group within the organisation concerned the First Principle of the Data Protection Act 1998 requires that this is made quite clear to would-be members. Paragraph 2 of Part II of Schedule 1 of the Act states that personal data are not to be treated as processed fairly unless certain information is provided to, or made readily available to, the data subject. The information specified includes the identity of the data controller, the purpose or purposes for which the data are intended to be processed, and any further information which is necessary, having regard to the specific circumstance in which the data are, or are to be processed, to enable processing in respect of the data subject to be fair. The fact that information relating to political religious or other belief, or membership of a trade union is now classified as sensitive data, means it is subject to more stringent controls than other personal data. It is important to make clear that we are not concerned with unfairness in relation to, for example, the benefit to a particular campaign. While some complaints, in relation to the Frank Dobson campaign did not appreciate the distinction, others were clear that their concern related to their details being more widely distributed than they had expected and, as a consequence had been used for internal campaigning purposes by a particular group within the membership, and could be used for other purposes.

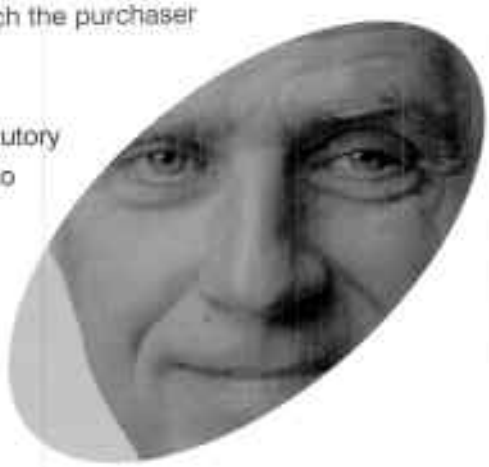


AVAILABILITY AND USE OF PUBLIC REGISTERS

In the UK there is a wide range of registers where the keeper of the register has, by law, to make the register available to the public and which include information about individuals. In many cases these individuals have no choice but to supply personal details for inclusion in the register, at least if they want to pursue a particular profession, business or other activity. The main registers include:

● The Electoral Register	Names and addresses of everyone over 18 who is eligible and has registered to vote
● The Register of Members ("Shareholders Register")	Names, addresses and shareholdings of members of companies.
● Register of Directors and Secretaries	Names, home addresses and other details of directors and secretaries of companies, including in some cases, date of birth.
● Register of County Court Judgements	Names, addresses and judgement details of those subject to County Court judgements.
● Register of Medical Practitioners	Names, addresses, sex and registration details of medical practitioners.

In most cases there is a sound public policy reason for the existence of a public register. For example, the Register of Medical Practitioners enables the public to check that those who claim to be qualified to practise medicine are so qualified. However the existence of a public register means that the information can be used for other purposes. For example, copies of the Register of Medical Practitioners can be purchased by pharmaceutical companies and used as a mailing list for marketing their products. The keeper of the register usually has no choice but to supply a copy regardless of the use to which the purchaser intends to put it.



The existence of a public register is generally based on long-standing statutory provisions. When Parliament decided to establish the register, the ability to use it for secondary purposes was restricted simply by its form. Without modern information systems the difficulty and expense of processing large numbers of paper records was a significant constraint. Developments in technology have largely removed this. Some registers are now sold in data form. The others, even if still sold in paper form, can be data captured quickly and cheaply, for example by using scanning equipment, and then processed for a variety of purposes.

In order to provide further information on the extent to which this is taking place we commissioned a 'Study of the Availability and Use of Personal Information in Public Registers'[1]. A summary of the results of the study is available on our website. One of the registers examined in the study is the Electoral Register. We have always had concerns that individuals are obliged to provide their details to the Electoral Registration Officer on penalty of a criminal offence and yet have no control over commercial uses of that information. These range from the compilation of direct marketing lists to credit referencing. We therefore welcome the Representation of the People Act 2000 which provides for two versions of the Register to be compiled, a full version for electoral purposes and a partial version from which individuals can opt-out of inclusion of their details. This partial version will be available to anyone who wishes to purchase it. This Act is a significant step forward in

1 Study of the Availability and Use of Personal Information in Public Registers; Final Report to the Office of the Data Protection Registrar; J C Davies and C Oppenheim; Loughborough University; Department of Information Science; September 1999; published at www.dataprotection.gov.uk

protecting privacy and we have been pleased to assist Home Office Ministers and their officials in bringing it to fruition. We now look forward to working with them to develop and implement the regulations that are needed to give effect to the Act's provisions.

One use of the Electoral Register has given rise to many complaints as well as much media interest. This is the compilation of a product known as UK Infodisc. This is available widely and cheaply on a CD-Rom as well as through the Internet. A version has even been given away free with a computer magazine. Although derived from the Register, UK Infodisc also includes other information such as telephone numbers. On the more expensive version of this product, reverse searching is possible. For example, by entering a telephone number a name and address can be found, by entering an address the names of those living at the address can be found. Further, where there is a telephone number listing at an address, the number can be linked to occupants who are not subscribers and who are not listed in other telephone directories. Potentially the way in which the product is compiled breaches both the Data Protection Act 1984 and the Data Protection Act 1998 but it is compiled outside the UK. We expect that in time the effect of the Representation of the People Act 2000 will be to deny the publishers of UK Infodisc and similar products access to the details of those who have opted out of inclusion in the partial version of the Electoral Register.

However the publishers of UK Infodisc have now launched a new product based on the Register of Directors and Secretaries. This claims to have the names, home addresses and telephone numbers, and dates of birth of more than 3 million Directors. We understand it also has details of co-occupants over the age of 18.

The study we commissioned did not, apart from notable exceptions for the Electoral Register and the Register of Members find widespread concern as to the availability and use of personal information in public registers. This was, at the time of the research, true of the Register of Directors and Secretaries, but we wonder how long it will remain so, given the advent of this new product. There is already evidence of some unease. Certainly the Institute of Directors has been reported in the press as having concerns about the product.

We have also received complaints in the past from those who had bought shares in the privatised utilities and who were surprised to receive a mailing from a political party soliciting support. More recently those holding shares in a company associated with research on live animals have received offensive mail from those opposed to such research, and, according to press reports, at least one shareholder found his home 'picketed' by demonstrators.

We also receive complaints from those who run businesses from home who object to receiving unsolicited mail as a result of the fact that the Mailing Preference Service is not designed to prevent unwanted business to business mailings.

These developments illustrate how quickly technology enables the personal information in public registers to be used in new and not always appropriate ways. Where individuals have no choice but to supply their personal details for inclusion in a public register, they should have the reassurance that there are effective controls in place to ensure the information can only be used to support the purpose for which the register was established. Where there are no controls or controls are ineffective, there must at least be a question over whether the

position is consistent with Article 8 of the European Convention on Human Rights relating to respect for one's private life which is given effect in the Human Rights Act 1998.

The Government has taken steps to restrict access to the full Electoral Register and we would welcome steps to apply comparable controls to other registers. In most cases this would mean a change in the law which should be introduced whenever suitable legislative opportunities are presented. The evidence of current wider use and concern may be limited but it is clear that it is increasing. We see it as important that steps are taken to protect those whose details appear in public registers now without waiting until their privacy is further eroded by the commercial exploitation of their personal information that developments in technology make possible.

PRIVATE SECTOR ISSUES

Consumer credit remains the largest category of complaint. Because of this, and as the use of credit reference information in the financial sector is extensive, with files held on virtually every adult member of the population, our work on credit referencing is a significant part of our work in dealing with the private sector.

CASE STUDY

Disclosure

A bank disclosed the details of a motor finance agreement to a car dealer without the complainant's consent. The car dealer in turn disclosed this information to the boyfriend of the complainant who had simply taken the car in for a service and had been asked by the complainant to make an enquiry about what cars might be available on a trade-in basis.

The complaint was raised with the bank, and the investigation revealed that the bank had disclosed details of the outstanding finance on the agreement to the dealer. The basis for the disclosure was that the customer's consent had been demonstrated by the dealer in providing the Bank with the customer's name and agreement number. However, the customer had not provided the dealer with this information. The Bank had not appreciated that some dealers would take steps to obtain such information from other sources, and as a result agreed to amend its procedures to raise this issue with its own staff and to ensure that dealers from whom it obtained business are made aware of their obligations under the Data Protection Act.

The implementation of the 1998 Act brought the right individuals have had under the **Consumer Credit Act** to access their credit reference files under the subject access provisions of the Data Protection Act. We hope that the new arrangements will maintain the advantage to the individual of being able to access their files at a lower fee (currently £2) and within a shorter time limit whilst improving security. Previously, the credit reference agencies had to respond to a request for a consumer file in seven working days. In practice this left little time for security checks to seek to ensure that the file was being sent to the data subject and not an impostor. The agencies are not under a duty to respond until they are satisfied as to the identity of the person making the request. This should increase security for individual's data and assist in the fight against fraud. Once checks are complete the file should be sent within the seven day period.

Similarly responsibilities for the arbitration of disputes between agencies and consumers over the "notices of correction" which individuals may place on their credit reference files moved to the Commissioner from the Director General of the Office of Fair Trading.

In agreeing as he did to this transfer, the Director General recognised the convergence of the work of our offices in the area of consumer credit disputes. This move will mean that consumers in the future will be able to approach one office for advice about both access and challenges to the accuracy of the data on their credit reference files. We would like to express our thanks to the Director General and his staff for the support they gave during the transfer period.

In order to reflect these and other changes for credit consumers the widely used leaflet **"No Credit"** was revised. It is now available through our office in English and Welsh and on audio cassette.

The issue of **third party data** is still under discussion with the credit industry. Reference was made in a previous report to the fact that the presence of this information on credit reference files remains a major source of complaint. This reflects concern that the practice invades the privacy of individuals and their families and that it is fundamentally unfair to take into account the behaviour of family members. Although, where there is no financial connection, there is the ability to disassociate the information of family members. Individuals usually only find out about this after credit has been refused.

In our discussions with the industry, including a working party made up of representatives of all of the major trade associations involved, we have made clear how seriously we view this matter. The Working Party are undertaking further research on the impact which the removal of third party data will have on their ability to lend responsibility. We understand that this is likely to mean a change in their lending practices and that they need to consider the issues involved carefully. We look forward to a satisfactory conclusion.

A significant proportion of the complaints we receive concern information filed with credit reference agencies by **credit grantors.** In July 1996 we began a process of consultation with interested parties with a view to establishing common standards for the filing of defaults in the interests of both consumers and those accessing credit reference records. In June 1999 we published a Guidance Note, "Defaults".

Interest in the new Act from the **trade credit sector** has continued, aided by seminars run by one of the major credit reference agencies. Discussions with the Factors and Discounters Association have been positive and they are now in a position to disseminate advice on the new Act which is specific to their industry.

A round of compliance visits to the major **catalogue mail order** companies has been completed this year. The aim was to address concerns particularly in relation to the provision of information to customers and credit reference practices as well as to give advice and assistance on the requirements of the new Act. The initiative was welcomed by the group. Whilst there are challenges to be met, for example, in the area of data quality, their response on the whole has been positive.

Last year several press articles highlighted a security issue for a number of high street banks and finance providers in that confidential waste was found in ordinary refuse bags left for collection in the street. Although all the organisations involved had procedures for the secure disposal of **confidential waste,** inevitably they rely on staff to follow them correctly.

What resulted was a review of practice and procedures by those concerned. A meeting also took place at the British Bankers' Association when problem areas and instances of good practice were shared. We believe a number of improvements have been made, such as the decision by most, if not all of the organisations involved not to segregate confidential and non confidential paper waste but to dispose of it all as if it were confidential. This is a bread and butter matter but which nevertheless goes to the heart of security issues. It also illustrates well that procedures alone are not sufficient to ensure compliance but that training, awareness and monitoring are necessary on an ongoing basis.

We described in last year's report our discussions with the Association of British Insurers about the development of a **database of insured drivers.** We continue to monitor developments as work on it progresses.

We also described our concerns about the motor version of the **Claims and Underwriting Exchange** (CUE). These have now been addressed, in particular through new customer notification and consent clauses to applicants for motor insurance, which provide information about the insured drivers' database and also, where relevant, about disclosures to CUE.

We gave some assistance to the **National Consumer Council** with its research into consumer awareness of and attitudes to uses of personal data and the resultant report '**Consumer Privacy in the Information Age**'.

Early in the year we completed a small compliance project to find out whether **internet service providers** had registered. We found that of our sample of thirty, ten were not registered. Of those, all except one registered when we drew to their attention the possible need to do so. Following investigation of the remaining business, it was decided not to prosecute, but they were advised that they should register.

We are represented at meetings of the Internet Users' Privacy Forum, a group representing both internet service providers and on-line civil liberties groups, which is working to draw up an "Internet Privacy Code" for internet service providers.

One important change early in the year was the introduction of the **Telecommunications Regulations** regarding the telecommunications sector and the use of the public telecommunication network. As well as creating rights for individuals in relation to unsolicited direct marketing phone calls and faxes, the regulations created new rights for companies in relation to unsolicited direct marketing faxes. Interim guidance on the Regulations was published in June 1999.

Individual subscribers who do not wish to receive unsolicited marketing calls can register their number with the Telephone Preference Service and subscribers who do not wish to receive unsolicited marketing faxes can register their number with the Fax Preference Service. The TPS and FPS act on the instructions of the Director-General of Telecommunications. Where those whose numbers are registered on TPS or FPS receive unsolicited marketing calls or faxes they may complain to TPS and FPS. We encourage them to do so, so that TPS or FPS can check that the numbers concerned are indeed accurately registered. These complaints are logged and the subjects of the complaint are written to and asked for an explanation. The TPS and the FPS then send us details of the complaints logged. This helps us identify those who appear to be continuing to make wholesale breaches of the Regulations.

Those who wish to complain about breaches of other provisions of the Regulations should do so directly to this office. The implementation of these Regulations has meant a significant increase in our workload in the office, and work on early formal enforcement action has been a priority. As mentioned in Chapter 4 such action has now commenced against a number of companies.

We continue to work closely with the Office of Telecommunications on a number of issues in this area including a code of practice in relation to the use of **caller line identification**.

We continue to liaise closely with the DTI regarding the implementation of the **Distance Selling Directive** which regulates the regulation of contracts which are concluded other than face to face.

RAISING AWARENESS

Responding to needs

In April each year we conduct our annual tracking studies to identify levels and trends in awareness of individual rights and responsibilities amongst data controllers and data subjects. These annual studies are conducted to provide us with an indication of the effectiveness of our communications and of equal value, an indication of how we can refine our communications strategies to better meet the needs of our publics.

This year we also built on the results of our guidance research by conducting a qualitative based study on how effective material produced by the Office is in providing data controllers with the information they need to comply with the provisions of the law.

Detailed results of our annual tracking studies and a list of key findings from the guidance study are available on our website.

Although public awareness of the Act decreased between 1997 and 1999, the level of public concern about the amount of information held by companies showed a sharp increase. We had planned to wait until the 1998 Act had been implemented before carrying out our advertising campaign, however, the tracking study findings suggested that we would need to maintain communications at a minimal level just to sustain awareness amongst data subjects.

Following on from the success of the previous distribution we therefore continued to use main Post Offices to distribute our 'Using the law to protect your information' leaflet. This channel has proved particularly effective for us in making more detailed and complex information available to the public. Over the period from October 1999 to March 2000 almost quarter of a million of these leaflets were distributed to the public. The leaflet itself was revised to achieve Plain English approval.

The implementation of the Telecommunications Regulations also presented us with an opportunity to communicate to the public about the identifiable issues of unsolicited telephone calls and fax messages. Previous experience has shown us that where issues are identifiable to the public and the message is complex, radio interviews provide us with an ideal medium through which to get the message across at minimum cost. In October, we therefore wrote to the news editors at local and regional radio stations, offering interviews covering these issues. As expected, take up was good and we gave 12 interviews. It is worthy of note that over a million people have now subscribed to the telephone preference bureau.

A new image

The implementation of the new law brought about a change in title to Data Protection Commissioner. With this provision within the law we planned to take the opportunity to bring in a new corporate identity for the Office upon implementation.

During 1999, however, it became more apparent that the proposed Freedom of Information legislation may require us to change the

Office identity again and within a short timescale. We therefore needed to develop an identity which could be used on a corporate level upon implementation of the Data Protection Act, but could also be used as a stand-alone brand, should the Freedom of Information proposals come about.

The resulting identity comprises a new symbol for data protection, which can be used on a corporate and brand level, a curved edge derived from the previous identity's shield, a new typeface and a range of formats for printed communications. In addition to the design elements, the new identity adopts many of the guidelines for accessibility. Where information is meant for a general market, we will endeavour to achieve Plain English, we will ensure availability in Welsh and we will make the information available in alternative formats for people with special needs.

Information and guidance

Throughout the year demand by data controllers for information on the new law has been high. We have continued to issue 'The Data Protection Act 1998 - An Introduction' at a rate of over 600 copies per week. In addition to this basic legal guidance, we have responded to the demand for a summary document on the key provisions of the new law. This leaflet, 'The Data Protection Act - A brief guide for data controllers', is now available from the Office, and is suitable for staff who process information on a day to day basis.

CASE STUDY

Default

An individual was unable to obtain a mortgage because of a default entry for several thousand pounds appearing on his credit file. The default related to an outstanding debt on a motor vehicle which the he maintained he did not owe. He complained to the Data Protection Registrar. In support of his complaints, he supplied a copy of a letter from the motor finance company which explained that they were prepared to come to an agreement in full and final settlement of the outstanding amount. However, he advised us that he was pursuing matters concerning the vehicle, which he claimed was defective, and the default registered against him, through the courts. The court hearing was scheduled for some months ahead.

The complaint was raised with the data protection contact at the finance company who advised that the individual had a genuine dispute about merchantable quality of the vehicle. He concluded that the default entry should not appear upon the individual's credit file and arranged for its removal.

We have spent a good part of the year developing and market testing the new training video. This has had a favourable response from data controllers who find it very useful for their staff induction programmes. Demand for the video has also been very high.

In March 2000 the Office took over responsibility for producing and distributing the 'No Credit' leaflet which was previously made available by the Office of Fair Trading. This leaflet is distributed directly to individuals and via a range of third parties to their customers. In view of the volume of leaflets distributed and the range of sizes of order, we have out-sourced this distribution to a local mailing house. Not only has this allowed us to take on board the work within our current staff resources, but it has also given us the opportunity to review our overall distribution mechanisms.

Getting the message across

One failing we have recognised with our current distribution systems, is that they rely heavily on individuals and organisations contacting us when they need information. Our longer term aim is to be more proactive in placing information at the point of need and in ensuring that the availability of our guidance material is as

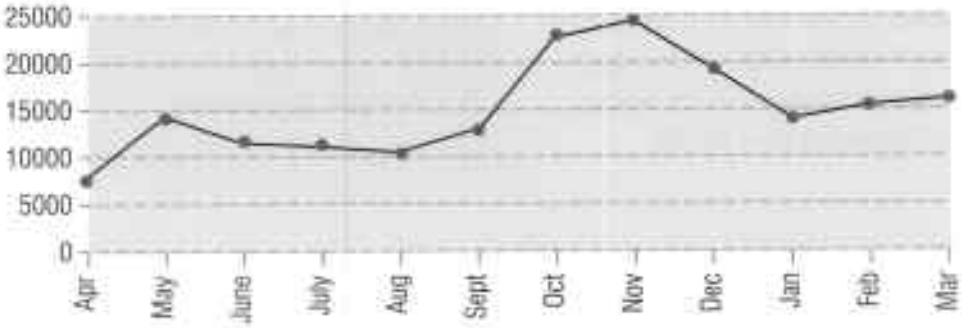
broad as possible. With this in mind, we have produced a range of posters for data controllers and advisory organisations to display on staff and public notice boards. The posters provide our website details and a telephone number for further information about the law.

We have also looked at a range of vehicles upon which we can 'piggy-back' our communications with those of third party organisations to achieve better value for money. In September 1999, we worked closely with the Judicial Studies Board to issue a guide to the law for Judges. Four thousand copies of the guide were distributed to all full and part time members of the Judiciary in England and Wales.

The changes in the provisions between the 1998 Act and 1984 Act will also require changes in our communication channels. The introduction of data held in other forms and the need to comply with the principles of good information handling by data controllers regardless of their need to notify, will impact upon many small and medium sized businesses, previously unaffected by data protection law. Whereas in the past we have issued communications to registered data users, in the future we will need to further exploit other cost-effective channels through which to target this wider group of data controllers. We are currently testing a range of vehicles through which to target the small and medium size business market.

Maintaining a presence

During the year we have continued to place our guidance material on our website. Following a review of the visibility of our site, we decided to change the website address to better reflect the content to www.dataprotection.gov.uk. The change in address in August 1999 may well have contributed to the sharp increase in hits on the Homepage during the following months.



More recently the website has been redesigned to fit with the new corporate identity and to comply with the government guidelines for websites. The new structure incorporates two dynamic applications, which allow us to update the advice and guidance and news and events sections directly from the Office. We have progressed some distance on the learning curve in maximising the effectiveness of the website in our overall strategy, but we are aware that we have some distance to go in ensuring we make optimum use of the medium in the longer term.

Investing in knowledge

For some time we have invested in educating children and younger people in their rights and in how they can take more control of their personal data by understanding these. This year work started on developing a schools pack for children in primary and secondary schools. The pack will contribute to the National Curriculum key stage levels 1 to 4 (ages 7 -15). The pack will be CD ROM based

and capable of being used on stand alone and networked systems to enable multiple individual or group use.

This year we also commissioned a group of students from the IT faculty at Salford University to produce a CD-ROM based training aid for IT and business students in higher and further education. The end product will need some refinement over the coming year before we launch it.

We have also reviewed the options for providing formal training seminars for data controllers. In the past these have been made available free of charge and on a commercial basis through a third party organisation. This year, although we have provided speakers for over one hundred seminars and conferences organised by third parties, we have prioritised our main resource into preparing for implementation and in developing guidance and compliance advice on the new law.

We are now developing a trial programme of on-line training for data controllers, which we plan to be available later in the year. The benefits to providing such training via the Internet are that it will be accessible to a far greater market at minimal cost and that we can provide modular training, which should more accurately meet the specific needs of the industry sectors.

Working with the media

We recognise the value of the public media in raising awareness and continue to invest in supporting media journalists and editors in covering data protection issues. Media interest has continued to grow and the number of media interviews has almost doubled this year. Our staff have been involved in over 500 public media interviews leading to 28 television and 66 radio appearances as well as a number of webcasts.

Empowering individuals - the information padlock

We have repositioned our marketing strategy this year to take account of the additional rights the new law brings for individuals. These new rights will further empower individuals to take more control and responsibility for their own personal information, and we have reflected this within our communications activity.

In November 1998 we ran a workshop on Individual Rights with a number of consumer representative bodies, the purpose of which, was to inform them of the developments brought about by the 1998 Data Protection Act and to extract ideas and feedback on our planned communications activity.

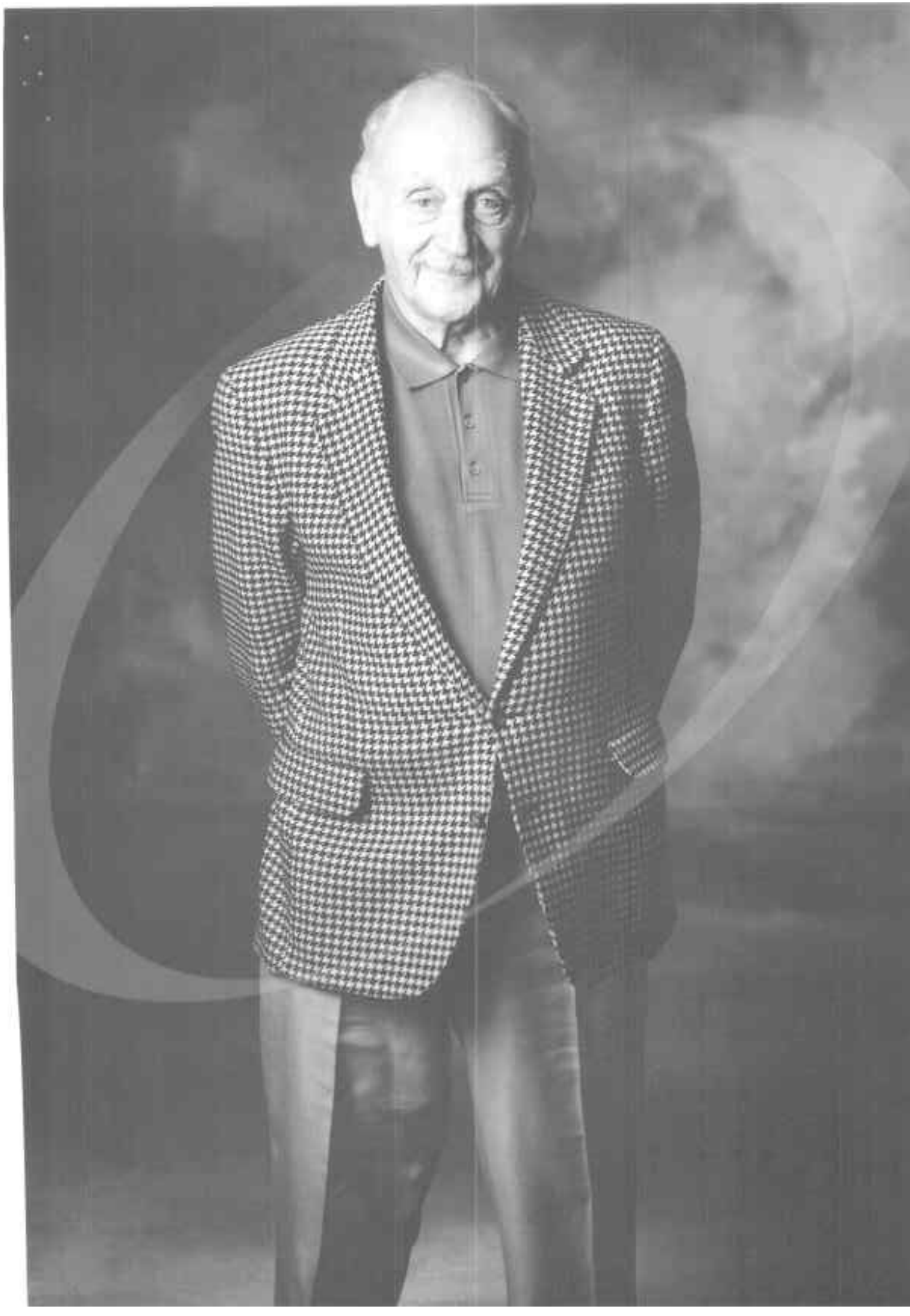
One idea discussed at this workshop was to introduce a national symbol (a signpost) which could appear whenever personal data was obtained, alongside which would be either an explanation of why the information was being collected, and how and by whom it would be used; or, a clear indication of where that information could be found.

On 30 March 2000 the Data Protection Commissioner and the National Consumer Council announced a joint initiative to improve public awareness of data protection issues relating to the collection and processing of individuals' personal data by launching this information signpost.

The new graphic signpost was unveiled to the general public by GMTV's Fiona Philips at the Data 2000 Conference at the London Hilton Hotel.

We believe that the responsibility for good information handling lies with data controllers and the introduction of this signpost is to make it easier for them to be open at the point of data collection. In turn, this should help individuals to see, at a glance, that their information is to be processed and for what purpose. With the benefit of this knowledge, they can go on to make choices about what information to provide and take steps to prevent any mishandling of it.

Posters and a leaflet explaining how the signpost should be used are available from our office and electronic copies of the signpost and leaflet can be downloaded from the website.



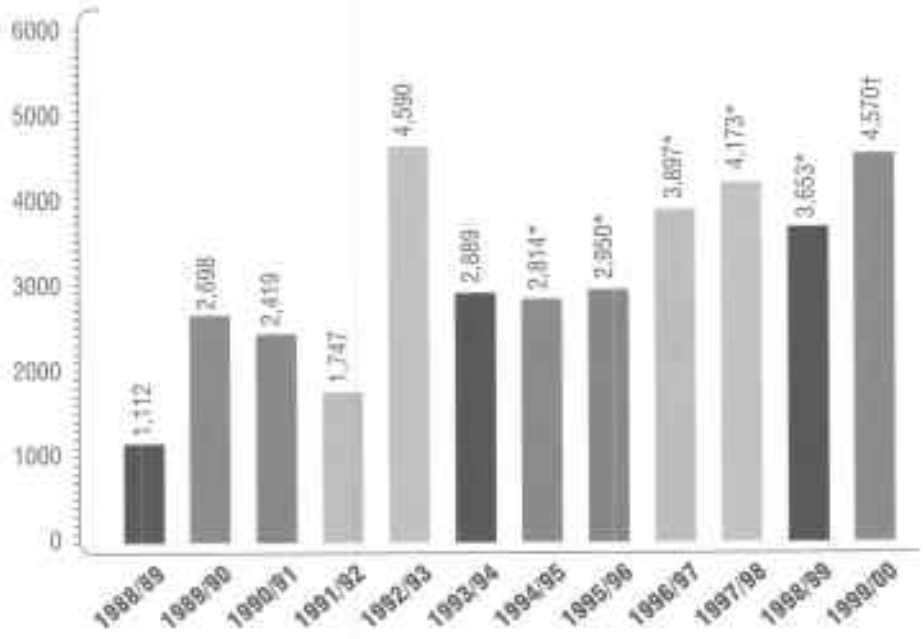
our annual caseload

COMPLAINTS

Under the 1984 Act, all individuals had the right to complain to the Registrar about misuse of information on computer. Complaints were dealt with by the sector teams in the Compliance Groups.

In the 11 months to the end of February we received 4,570 complaints - pro-rata more than we have previously received in any full year. Adjusted pro-rata this represents a 36% increase on the previous year. Coming at a time when there has been an increased work-load generated by queries regarding the new Act, and the development of new procedures, this has placed a huge burden on compliance staff. Unfortunately, but understandably, this has led to substantial back-logs.

Total complaints received 1988 to 2000:



* Figures since 1994/95 refer to the financial year commencing 1 April and ending 31 March rather than using the previous reporting period for the Annual Report which ran from 1 June to 31 May.

† This figure for the financial year 1999/2000 is for complaints received for the eleven months to 29 February 2000 inclusive. Complaints received from 1 March 2000 have been handled as requests for assessment.

Complaints handled during the eleven months to 29 February 2000

cases investigated	45%
cases not investigated*	55%

* These are cases which are not pursued individually with a data user because they are better dealt with through the provision of information or advice or because they relate to issues being addressed on a wider basis.

Complaints were received about:

Direct Marketing	18%
Consumer Credit	31%
Other	51%

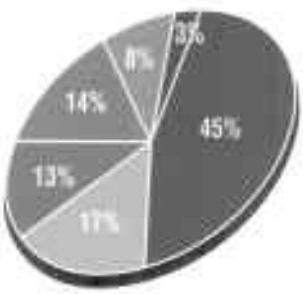
Regulations implementing the provisions of the EU Data Protection Telecommunications Directive 97/66/EC came into effect with the 1998 Data Protection Act. The Commissioner is responsible for enforcing these regulations. Since May 1999, we have received over 650 complaints under these regulations.

Many complaints raising data protection concerns require our compliance officers to request further information from the complainant and the organisation being complained about. This with the varying complexity of the cases themselves results in the time taken to investigate complaints varying considerably.

Of the 1,812 complaint files closed:

- were open for more than 12 months 14%
- were open for 6-12 months 21%
- were open for 3-6 months 34%
- were open for 0-3 months 31%

Outcome of investigated cases:



- direct remedy for complaint 45%
- not followed up 17%
- indirect remedy for complaint 13%
- not upheld 14%
- no action necessary 8%
- not covered by the Act 3%

CASE STUDY

Employee resigns after accessing colleague's personnel information

An employee of a further education college complained to the Registrar that other employees, outside the Personnel Department, were able to access confidential personnel information about her.

The complainant explained that any member of staff on the network neighbourhood system could access documents concerning her, including a memo, which set out a number of concerns she had raised with her line managers. She said that a member of the Personnel Department who had saved them without any password protection and in an open directory had typed these documents. The complainant said that at least seven employees on the network system could have had access to these files, one of which was entitled 'Ms X's claim for extra pay'.

The complaint was pursued with the college's Data Protection Officer, who confirmed that documents concerning the complainant had been accessed by a member of staff not involved in the personnel function of the college. The member of staff concerned had deliberately accessed information in a folder on the central file server. In view of the fact that she had acted in breach of the terms and conditions of her employment she had resigned. Her supervisor had also been disciplined.

The Data Protection Officer explained that as soon as the matter had come to light the steps had been taken to immediately password protect the documents in question and all other relevant documents at document level. At a general staff meeting held after the event additional training was provided for staff to remind them of the principle of confidentiality and the need to password protect sensitive information to prevent a recurrence of the events which led to the complaint.

Depending on the findings or where a criminal offence is alleged, complaints may be passed to the Investigations Department for further action. Data Protection Investigators have made 587 visits to premises this year in the course of their investigations into alleged criminal breaches of the Act.

SEARCH WARRANTS

Applications were made, and no-notice search warrants granted, in respect of eleven premises. In the main, the investigations centred on, and the evidence sought in respect of, the unlawful procurement of information by private investigators and tracing agents.

	1995/96	1996/97	1997/98	1998/99	1999/00*
Cases considered for prosecution	57	-	118	215	125
Visits to business premises	710	603	471	700	388
Visits to dwellings	246	322	313	319	199
Witness statements obtained	317	382	378	433	346
Interviews conducted under caution	104	176	136	216	098
Cases convicted	33	60	38	55	130

ENFORCING THE ACT

Prosecutions	1993/94	1994/95	1995/96	1996/97	1997/98	1998/99	1999/00*
Number of offences charged	36	61	39	67	38	59	145
Number of offences resulting in acquittal or withdrawn	3	2	5	8	0	4	15
Number of offences resulting in finding of Guilty	27	41	32	58	38	55	130

125 cases were submitted to the Legal Department for consideration of prosecution. 145 cases proceeded to court and 130 of them resulted a finding of Guilty.

Convictions	1999/00
Unregistered data users	28
Cases of unlawfully procuring information	91
Cases of selling unlawfully procured information	–
Cases of data users 'using' data for unregistered purposes	7
Employee for using data for an unregistered purpose	–
Data user for disclosing data	–
Employee for disclosing data	–
Directors conniving offences by company	4

Enforcement	1995/96	1996/97	1997/98	1998/99	1999/00
Preliminary Registration Refusal Notices	1	–	–	–	–
Preliminary Registration Refusal leading to Registration Refusal	0	–	–	–	–
Registration Refusal Notices	31	0	–	–	–
Preliminary Enforcement Notices	4	6	19	7	5
Preliminary Enforcement Notice leading to Enforcement Notice	1	–	3	2	–
Enforcement Notices	3	2	5	5	1
Preliminary Transfer Prohibition Notices	1	–	–	–	–

This year we served five Preliminary Enforcement Notices and one Enforcement Notice. One Preliminary Notice remains pending and may result in formal enforcement action in the future. No formal enforcement action was taken this year in respect of the four Preliminary Notices, which remained pending at the beginning of this year.

PROSECUTIONS FROM 1 APRIL 1999 TO 31 MARCH 2000

Defendant	Section	Magistrates Court	Date of Hearing	Result	Fine (£)	Costs (£)
Coldseal Limited	5(1)	Ilkeston	01.04.99	Guilty	150.00	763.39
Dome Cosmetics Limited	5(1)	Acton	01.04.99	Guilty	1000.00	655.59
Gordon William Henderson t/a Video Express	5(1)	Truro	01.04.99	Guilty	Absolute Discharge	0.00
World Trade Conferences Limited	5(1)	Highbury Corner	09.04.99	Guilty	1000.00	675.00
Mark Williams	5(1)	Cardiff	15.04.99	Guilty	200.00	250.00
Mukhtar Singh Gorsya t/a One Stop	5(1)	Chatham	16.04.99	Guilty	25.00	150.00
C Manning partner Killik & Co	5(2)(b)	Horseferry Road	19.04.99	Guilty	Absolute Discharge	500.00
C Manning partner Killik & Co	5(2)(b)	Horseferry Road	19.04.99	Guilty	Absolute Discharge	
Southco Europe Limited	5(1)	Worcester	26.04.99	Guilty	100.00	900.00
Darren Brady t/a Accommodation Outlet	5(1)	Bow Street	27.04.99	Guilty	100.00	250.00
Sarah Taylor	5(6)	Coalville	28.04.99	Guilty	100.00	0.00
Cannon & Co Solicitors	5(1)	North West Surrey	30.04.99	Guilty	250.00	753.00
Stephen Toon as director of Skywood Limited	20(1)	Chesterfield	06.05.99	Guilty	500.00	250.00
Stephen Toon as director of Bannerwood Limited	20(1)	Chesterfield	06.05.99	Guilty	500.00	250.00
Martin Paul Ely t/a Ely Consultancy Services	5(1)	Swaffham	10.05.99	Guilty	200.00	225.00
Sitel UK Limited	5(1)	Banbury	13.05.99	Guilty	2000.00	793.13
Ros Raynes	5(6)	Leamington Spa	25.05.99	Guilty	100.00	125.00
Alan McGovern	5(6)	Leamington Spa	25.05.99	Guilty	100.00	125.00
William Murphy	5(6)	Marylebone	07.06.99	Guilty	260.00[1]	100.00

Defendant	Section	Magistrates Court	Date of Hearing	Result	Fine (£)	Costs (£)
Beverley Ann Knox t/a R&B Consultancy Services	5(6)	Swaffham	08.06.99	Guilty	2000.00	–
Beverley Ann Knox t/a R&B Consultancy Services	5(6)	Swaffham	08.06.99	Guilty	2000.00	1478.96
Bowman Leisure Limited t/a 001 Taxis	5(1)	Oxford	11.06.99	Guilty	1250.00	1081.07
Darren Anthony Young t/a Direct Security Alarms	5(1)	Bromley	28.07.99	Guilty	Conditional Discharge	293.75
Derek Hinton t/a Direct Security Alarms	5(1)	Bromley	28.07.99	Guilty	Conditional Discharge	293.75
Butlins Limited	5(2)(b)-P001	Hemel Hempstead	29.07.99	Guilty	1500.00	894.38
Butlins Limited	5(2)(b)-P004	Hemel Hempstead	29.07.99			
Butlins Limited	5(2)(b)-P008	Hemel Hempstead	29.07.99			
Butlins Limited	5(2)(b)-P013	Hemel Hempstead	29.07.99			
Butlins Limited	5(2)(b)-P015	Hemel Hempstead	29.07.99			
Perry Keena	5(6)	High Wycombe	04.08.99	Guilty	2500.00	1391.00
Mooodance Media Limited	5(1)	South Western	12.08.99	Guilty	3500.00[3]	592.00
Apex Computer Recruitment (UK) Limited formerly IT Prospects Limited	5(1)	Kingston	16.08.99	Guilty	3000.00	681.50
Hitachi Credit (UK) plc	6(5)&5(2)	Feltham	07.10.99	Discontinued	0.00	0.00
Hitachi Credit (UK) plc	5(2)(b)	Feltham	07.10.99	Discontinued		
Hitachi Credit (UK) plc	5(2)(b)	Feltham	07.10.99	Discontinued		
Hitachi Credit (UK) plc	5(2)(b)	Feltham	07.10.99	Discontinued		
Hitachi Credit (UK) plc	5(2)(b)	Feltham	07.10.99	Discontinued		
Hitachi Credit (UK) plc	5(2)(b)	Feltham	07.10.99	Discharged		
Rail Europe Limited	5(1)	City of London	10.11.99	Guilty	1500.00	587.50
Viking Star Limited t/a Edward Knight	5(1)	West Suffolk	15.11.99	Guilty	750.00	719.20
David Spencer	20(1)	West Suffolk	15.11.99	Guilty	500.00	690.00
Heath Rainsden	20(1)	West Suffolk	15.11.99	Guilty	500.00	690.00
Playmate Escort Services Limited	5(1)	Nottingham	22.11.99	Guilty	Conditional Discharge	1500.00

Defendant	Section	Magistrates Court	Date of Hearing	Result	Fine (£)	Costs (£)
Trevor Browne t/a Blue Diamond	5(1)	Eastbourne	30.11.99	Guilty	700.00	694.00
London Calling Music Limited	5(1)	Greenwich	02.12.99	Guilty	300.00	376.00
Telecom Billing Systems Limited	5(1)	Staines	07.12.99	Guilty	1300.00	771.54
Barry Graham Wilson t/a Hill Taylor Telemarketing	5(1)	Exmouth	14.12.99	Guilty	100.00	100.00
Ian Andrew Taylor t/a Hill Taylor Telemarketing	5(1)	Exmouth	14.12.99	Guilty	100.00	100.00
The Rugby Football Union	5(1)	Brentford	14.01.00	Guilty	1500.00	932.22
Culvers Macclesfield	5(1)	Macclesfield	26.01.00	Guilty	250.00	250.00
Eric Pickles	5(6)[4]	Dewsbury	26.01.00	Guilty	300.00	765.85
Eric Pickles	5(6)[4]	Dewsbury	26.01.00	Guilty	300.00	
Eric Pickles	5(6)[4]	Dewsbury	26.01.00	Guilty	300.00	
The Baby Grand Hotel Co Limited	5(1)	Leeds	16.02.00	Guilty	500.00	547.52
Somer Community Housing Trust	5(1)	Bath	21.03.00	Guilty	500.00	300.00
Nottinghamshire Probation Committee	5(1)	Derby	23.03.00	Dismissed		

1. In addition, in 10 cases prosecutions were withdrawn.
2. Mr Murphy appealed against the conviction. The Appeal was heard on 6 August at Blackfriars Crown Court. The Appeal was dismissed and the conviction confirmed. The costs were increased to £1200.00 for the Appeal.
3. Appeal against sentence at Kingston Crown Court - fine reduced to £1000.00.
4. 81 similar offences taken into consideration.

REGISTRATION DEPARTMENT STATISTICS

The Data Protection Register	1996/97	1997/98	1998/99	1999/00
Register Entries	212,943	224,909	229,693	243,681
Registered Data Users	200,864	211,992	225,440	237,146*
New Applications	19,197	21,591	23,202	25,012
Renewal Requests	39,647	33,522	67,205	38,354
Re-applications Submitted	9,396	8,192	10,382	8,220
Requests for Amendment	29,766	22,079	28,528	25,047
Notifications Received	–	–	–	3,260

* extrapolated

OUTPUT MEASURES AND PERFORMANCE INDICATORS FINANCIAL YEARS 1998/1999 TO 2001/2002

	Actuals		Estimates and Targets	
Registration and Notification	1998/99	1999/2000	2000/2001	2001/2002
Number of weighted transactions processed	226,400	212,033	194,599	244,913
Number of weighted transactions processed per officer per day	48.74	47.02	50.76*	57.49*

* Dependent on increased staffing to handle current level of telephone calls

There were four 'products' in Registration - applications, renewals, re-applications and changes. There is still Registration work to be completed. Initially for Notification there will be applications, and transformations from registration renewals to notifications, which will continue until 28 February 2003. During Quarter 4 of 2000/2001 renewals will begin. It is also anticipated that changes to notification entries will be received by the Office. Each product is weighted in accordance with its processing time to enable year-on-year comparisons of performance to be made, reflecting the differing workloads encountered. The 'processed per officer day' figures incorporate different staff levels from year to year, and encompass increased productivity targets. Estimated weightings have been used for the Notification system introduced on 1 March 2000.

	Actuals		Estimates and Targets	
Complaints and Assessments	1998/99	1999/2000	2000/2001	2001/2002
Received	3,653	5,166	5,000	5,000
Not Investigated	1,766	2,227	2,150	2,150
Investigated and Closed	1,686	1,812	2,851	2,851
Number closed per officer day	0.79	0.74	0.92	0.92

The number shown is the total number of complaints received by the Registrar (now the Commissioner) although not all have required detailed investigation. From FY 2000/2001 the table also includes estimated requests for Assessments. The table does not distinguish complaints made under the 1984 Act and requests for assessments under the 1998 Act.

	Actuals		Estimates and Targets	
Contact with our customers	1998/99	1999/2000	2000/2001	2001/2002
Telephone Enquiries received	48,549	55,070	55,000	55,000
Calls received per line hour	8.80	8.72	8.72	8.72

Telephone enquiry figures are the calls received by the 'Information Line'. The proportion of calls dealt with by the Information Line has been reduced in recent years by the introduction of 'auto attendant' facilities. Some calls which would have previously gone to the Information Line are now redirected to other extensions, principally in Registration (now Notification) and Marketing. It is anticipated that the number of calls will be increased further by the discussions about and the enactment of the Freedom of Information Bill. The target figures for the "calls received per line hour" are based on further efficiency improvements which will be set as a target. However, achieving year on year gains of this nature will become harder as at least two lines are kept open for 8 hours each day because of the volume of incoming calls currently being received. "Line hours" are the hours spent by staff receiving incoming telephone calls on the Information Line.

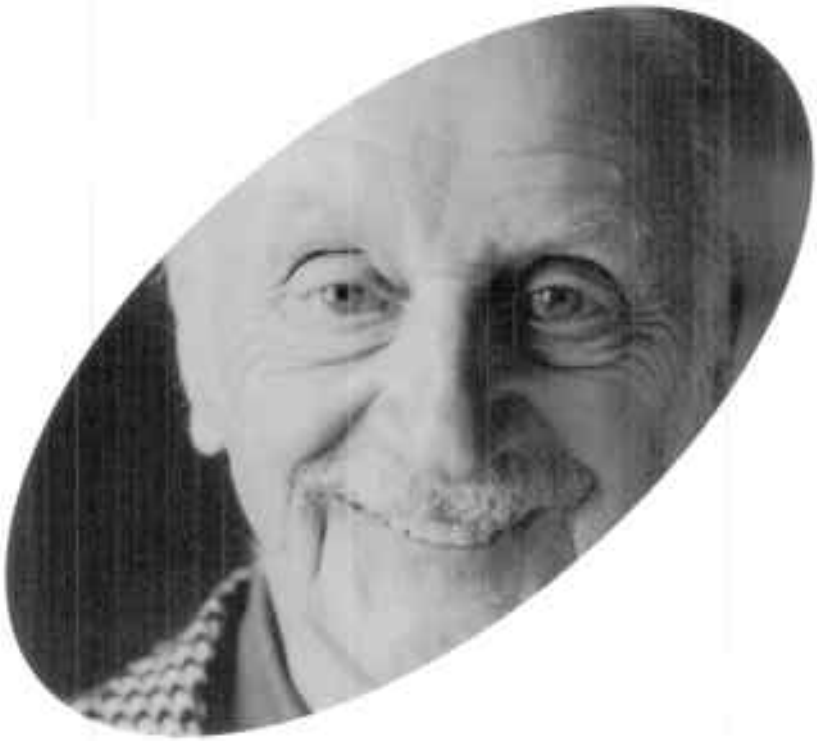
	Actuals		Estimates and Targets	
Public Awareness	**1998/99**	**1999/2000**	**2000/2001**	**2001/2002**
% large data controllers aware of subjects' rights	81	77	82	82
% small data controllers aware of subjects' rights	51	58	51	52
% data subjects aware of own rights	21	14	25	25

The figures are based on annual tracking research with projections for future years.

Notes:

1. If the Freedom of Information Act gives right of access to individuals from 2002/2003, this will have a significant impact on the OMPIs set for that year.

2. Anyone requiring more detailed statistics and information is welcome to apply to the Office.



a wider perspective

FREEDOM OF INFORMATION

Last year's Annual Report recorded the publication on 24 May 1999 of the draft Freedom of Information Bill for pre-legislative scrutiny and public consultation. Our early written comments, which were included at Appendix 6, provided our formal response to the consultation exercise.

The Committees of the House of Commons and House of Lords which considered the draft Freedom of Information Bill reported in July. The Government responded in October and at the same time also published information about responses to the consultation exercise.

The Freedom of Information Bill received its First Reading in the House of Commons on 18 November 1999. At the time of writing (early May) the Freedom of Information Bill is before the House of Lords with a date for Committee Stage yet to be announced. Key stages in the legislative progress of the Freedom of Information Bill to date are set out in the accompanying table.

Freedom of Information Bill legislative progress

House of Commons	
17 November 1999	Queen's Speech – Announcement of FOI Bill in Legislative Programme for session 1999/2000
18 November 1999	First Reading FOI Bill published (Bill 5)
7 December 1999	Second Reading
21 December 1999 to 10 February 2000	Committee Stage
10 February 2000	Amended FOI Bill published (Bill 66)
4 & 5 April 2000	Report Stage
	Third Reading
House of Lords	
6 April 2000	First Reading Amended FOI Bill Published (HL Bill 55)
20 April 2000 date to be announced	Second Reading Committee Stage

There have been changes to the Freedom of Information Bill from the draft version and during its progress through the legislative process but the approach to providing access to personal information remains unchanged. Decisions on disclosure of personal information will involve reference to the Data

Protection Act 1998. The Freedom of Information Bill proposes amendments to the Data Protection Act 1998. These are principally for the purpose of providing access to all personal information held by public authorities. Other proposed amendments include extending the scope of the Data Protection Act 1998 to the processing of personal data by or on behalf of either House of Parliament.

The Government's proposal that the Information Commissioner should oversee both the data protection and Freedom of Information regimes would have major implications for the organisation of this office. As indicated in Chapter 2 we have given some thought to how this should be achieved and will be ready to take on new responsibilities two months after Royal Assent if the Bill is enacted as the Government intend. In the meantime the Home Office has provided specific funding to enable essential work arising from the Government's proposals for introducing Freedom of Information, and which is consistent with our existing remit, to be undertaken by this office. We are pleased to have been able to continue to make the experience and expertise of this office available to those working on the Freedom of Information proposals. We have added a Freedom of Information section to our website.

It is clear that the approach of those working in the public sector will be crucial to the effective implementation of the Freedom of Information legislation. Last year's report recorded that an Advisory Group on Openness in the Public Sector had been established by the Home Secretary and that the Registrar was a member of that Group. The purpose of the Advisory Group was to 'advise the Home Secretary on the steps needed to be taken ahead of legislation notably to bring about a culture of greater openness in the public sector'[1]. The Group concluded its work under the chairmanship of Mike O'Brien, Parliamentary Under-Secretary of State for the Home Office, and published its report in December. The Report contains the Advisory Group's recommendations for a strategic approach to increasing openness before and after the legislation is passed.

FOI Scotland

On 25 November 1999 the Scottish Executive published 'An Open Scotland, Freedom of Information, A Consultation'[2], which set out for public discussion broad proposals for a statutory freedom of information regime for devolved Scotland. The proposals include the establishment of a new office of Scottish Information Commissioner to promote and oversee that regime. The Data Protection Act 1998 provides for access by data subjects to their personal data held by Scottish public authorities. It is proposed that the Scottish Freedom of Information legislation will provide for access to personal information held by Scottish public authorities where this is not provided for by the Data Protection Act 1998. Clearly the boundary issue associated with the interface between the data protection and the Scottish and UK Freedom of Information regimes will need to be addressed, and there will be a need for effective liaison between the Scottish Information Commissioner and the Data Protection Commissioner/Information Commissioner. We have had useful preliminary discussions with Scottish Executive officials and, as was made clear in our formal response to the consultation paper[3], we look forward to helping lay the foundations for a future constructive relationship between this office and that of the Scottish Information Commissioner.

Footnotes

1 Advisory Group on Openness in the Public Sector, Report to the Home Secretary, December 1999, paragraph 1.5

2 'An Open Scotland, Freedom of Information, A Consultation', (SE/1999/51) Edinburgh, The Stationery Office 1999

3 'Response of the Data Protection Commissioner, An Open Scotland, Freedom of Information', March 2000

REGULATION OF INVESTIGATORY POWERS BILL

The Government's Regulation of Investigatory Powers Bill is now before Parliament. A paper setting out our views on the draft legislation has been prepared for parliamentarians. Broadly we are concerned that warrants for interception of communications and other forms of surveillance are available through administrative rather than judicial procedures and that forms of surveillance which are equally intrusive are treated differently. In this context, we are particularly concerned that the Bill appears to allow access to encrypted electronic information without a warrant, simply on the basis of a notice issued by a specified law enforcement authority. We contend that this notice should only be served where a judge or another independent authority has ruled that there are grounds for approving its issue. Our concerns about the Regulation of Investigatory Powers Bill are linked to our concerns about various international initiatives to combat cybercrime (see Chapter 8).

STANDARDS AND CULTURE

We have long held the view that data protection cannot be achieved by reactive policing. What is required is a culture change so that all are aware of the need to protect the privacy of individuals. Systems specifiers, purchasers, designers and suppliers should then take proper account of individual privacy when implementing system changes.

We have promoted several initiatives with that objective in mind. Our programme of educational materials for schools, our project to develop data protection design standards are all part of this approach. We have particularly given active encouragement to those bodies seeking to develop standards, codes and compliance tools. We want organisations to own the privacy protection problem and also own the solutions.

Consequently, we have been particularly pleased in the last year to see the development of a Code of Practice at a European level by ICX to help all data controllers to comply with Directive 95/46/EC, but especially those companies who operate across borders and transfer data outside the European Union. We provided comments on a draft of the Code and were represented at its launch in the Hague on 15 December 1999. We hope that the work on this Code will be taken forward to provide greater added value by specifying more precisely what steps company managers should take to implement and comply with the rules of Directive 95/46/EC.

At the International Conference in Hong Kong, the Deputy Commissioner gave a presentation on our support for standards to assist the implementation of data protection requirements. Standards could either address behavioural and quality issues or deal with more traditional matters such as system design. We have consequently supported the initiative of CEN/ISSS in looking at the role of standards in supporting the implementation of Directive 95/46/EC. We have been represented at several CEN/ISSS meetings during the last year and the Deputy Commissioner repeated his Hong Kong presentation for an explanatory workshop organised by IPTS in Seville during October 1999. The European Commission has given a formal mandate to the European standards bodies including CEN/ISSS to look at the role of standards in this area. We see this as a valuable initiative to integrate formal law and self regulatory machinery and we support this co-regulatory approach demonstrated by the European institutions. Following the CEN/ISSS Open Seminar in March 2000 we expect to take part in further work supporting the development of both Codes of Practice and technical standards by commercial companies and other organisations seeking to implement good data protection practice.

British Standards Institute

Our office has been closely involved in work with the British Standards Institute, co-operating with them in the publication of the their loose-leaf general 'Guide to the Practical Implementation of the Data Protection Act 1998'. The main aim of this product is to add value to existing guidance on the new law by incorporating practical suggestions on compliance. The guide is produced in loose-leaf format to allow targeted up-dates on specific areas to be added easily. An up-date on the data protection issues arising from the use of electronic mail has recently been published. A series of further additions are planned. Our involvement in this project is linked to our participation in the work of the European Standards Institute CEN/ISSS.

CASE STUDY

Unlawful procurement

A woman unlawfully procured registered keeper details from the DVLA concerning a vehicle, the driver of which had been seen in the company of her estranged husband. Following prosecution she was fined.

CODES OF PRACTICE

Our own legislation gives the Commissioner a duty to promote good practice and, in certain circumstances issue, consider or disseminate codes of practice in order to fulfil this duty.

Where the Secretary of State so directs by order, or where the Commissioner herself feels it appropriate, she can prepare and disseminate codes of practice. She is also required to encourage trade associations to prepare codes, where appropriate, and to consider codes submitted by trade associations as to their promotion of good practice. The Act provides that 'good practice' may include practice which the Commissioner considers desirable, even if not actually necessary for compliance with the law. A Code of Practice must provide added value to the provisions of the Data Protection Act 1998 by specifically focusing on the data protection questions and problems in the area or sector to which it is intended to apply.

Where the Commissioner issues or considers codes of practice a consistent approach to the evaluation or production of such codes should be adopted. Standard procedures must be followed in the development of such codes although the subject matter and application of the codes may differ. With this in mind we developed a 'control document' to set out broad guidelines as to how codes of practice should be produced or considered and approved and how compliance with our statutory obligations can be ensured.

Our first code of practice is aimed at users of CCTV (closed circuit television) and similar surveillance equipment who monitor, and record images from, those areas to which the public have largely unrestricted access such as town and city centres and streets, and the public parts of shops and shopping centres. The code applies to schemes which are used for the general purpose of crime prevention and detection, and public safety. It is not intended that this code should cover targeted surveillance activities by official law enforcement bodies, which will be covered by the forthcoming Regulation of Investigatory Powers Bill. The code sets data protection standards for all aspects of CCTV surveillance operations ranging from the siting of cameras, to how long the images are held for before destruction. This code is published today and we hope it will establish consistently high standards among CCTV operations and that public confidence in the widespread use of such surveillance technology will be maintained.

The second code we are preparing is to cover the use of personal data in employment relationships. We have noted a particular demand for guidance in this area amongst data controllers, possibly a reflection of the fact that the 1998 Act brings structured manual records containing personal data, including employee

personnel files, within the scope of data protection law for the first time. Surveillance in the workplace is becoming increasingly common. Technological advances have made it easier for employers to monitor their employees' behaviour. The research to underpin this was published last year. We expect to consult on the code itself in the autumn.

AUDITING DATA PROTECTION COMPLIANCE

We have also undertaken a project to develop an audit methodology manual, which is aimed at providing data controllers with a tool to enable them to assess their compliance with the requirements of the data protection legislation. It is intended that the manual will provide guidance for all data controllers whatever their knowledge of auditing or data protection. The manual is currently in draft form, but it has been tested during five pilot exercises and has been subject to peer review by the Home Office auditors. The draft is being reviewed in the light of comments received and will then be made available for use by data controllers and by the Commissioner's staff when asked to carry out compliance audits by data controllers.

INTERNET AND E-COMMERCE

The Data Protection Act 1998 applies to the processing of personal data over the Internet in the same way as it applies to the processing of data by more traditional automatic means. Although the same data protection rules apply, the Commissioner recognises that organisations and individuals may find it difficult to envisage what steps they should take to ensure that they comply with their data protection obligations in the on-line environment. We have recently produced guidance for data controllers in this area. In the light of the development of e-commerce, we have been particularly concerned to provide advice to organisations who use websites to facilitate their business activities.

Trust UK Limited is a joint non-profit making venture between the Alliance for Electronic Business, comprising five leading business associations, and the Consumers' Association, endorsed by the UK Government. It seeks to foster consumer trust and confidence in Internet trading through the accreditation of on-line codes of practice. Codes must require subscribers to abide by the Data Protection Act 1998. We participated in a Working Party that co-ordinated the development of the accreditation scheme.

In October 1999 we commented on the Department of Trade and Industry's White Paper 'Modern Markets: Confident Consumers'. Amongst other things the white paper sets out an agenda to provide people with the skills and information they need to become demanding consumers and to encourage good business practice in the context of new global markets and the development of e-commerce. We welcome measures that will mean that individuals are better informed when making decisions as consumers, as this will often aid their understanding of how their personal data is processed. We also welcome measures that will improve the public's understanding of consumer and individual rights, develop effective complaint handling procedures within businesses, and encourage the drawing up of consumer codes of practice for e-commerce. We also commented on the Government's draft legislation to facilitate the use of electronic communications and electronic data storage as set out in the DTI consultation paper 'Promoting Electronic Commerce'. However, the provisions within the draft legislation on which we commented, namely the measures relating to the investigation of protected electronic data, have subsequently been taken out of this Bill and been incorporated into the Regulation of Investigatory Powers Bill.

the international dimension

ARTICLE 29 WORKING PARTY

The Article 29 Committee, set up under the EU Data Protection Directive to advise on data protection issues arising at a European level, continues to take up an increasing amount of our time. Recent discussion on the committee has been dominated by the ongoing negotiations between the US Department of Commerce and the European Commission on the American proposal to establish a 'safe harbor' for the transfer of personal data to the USA from the EU.

The committee produced 14 formal opinions and recommendations in the year to the end of March 2000. A variety of different topics were addressed, including 'safe harbors', the level of personal data protection in certain non-EEA states, and relevant issues in the telecommunications sector and on the Internet.

We have contributed to the work of two sub-groups of the Article 29 Committee: one group liaising with the Federation of European Direct Marketing in their production of a European code of conduct for direct marketers compliant with the Data Protection Directives; the other considering model contract clauses as a means of achieving adequacy for the purposes of transborder data flows, submitted to the European Commission by the International Chambers of Commerce.

BERLIN TELECOMMUNICATIONS WORKING GROUP

We continue to be represented at meetings of the Berlin Telecommunications Working Group. This group meets twice a year to consider telecommunications related issues. Attendees include staff of both EU and non-EU data protection authorities as well as other experts in the field. The Berlin Commissioner acts as Secretariat for the group.

MEETINGS OF COMMISSIONERS

This year's annual International Commissioners' Conference was held in Hong Kong. This forum for international co-operation once again addressed a variety of issues, notably the data protection and privacy implications arising from the continued development of the Internet and other networks. We led the debate on the development of self-regulation at international level. There is a pressing need to develop internationally accepted ways of securing respect for personal privacy, for example through standards and codes of practice, because of the inherently global nature of e-commerce and the problems of applying rules of particular jurisdictions.

In April of this year we attended the annual European Data Protection Commissioners' Conference in Stockholm. The Commissioners discussed the data protection implications involved in the development of genetic databanks, a topic brought sharply into

focus by the creation of a national database of genetic information in Iceland. They agreed to accept the conclusions and recommendations of our paper analysing the data protection and privacy issues associated with various international initiatives to combat cybercrime. The Commissioners also discussed complaints handling, privacy audits and relevant issues arising in the telecommunications sector and on the Internet.

Conferences with the Commissioners representing Guernsey, Jersey, The Isle of Man and the Republic of Ireland continue to be held twice yearly. The primary purpose of these meetings is to update the small island data protection authorities on current data protection concerns. This is particularly important at present as many of these jurisdictions are redrafting their data protection legislation to reflect the provisions of the EU Data Protection Directive. Meetings were held in Wilmslow in October 1999 and in the Isle of Man in May 2000.

COMPLAINTS HANDLING

The EU Data Protection Directive requires that supervisory authorities co-operate with each other in order to perform their duties. At their European Spring Conference in 1999 the Data Protection Commissioners agreed that it would be helpful to hold a workshop to compare different national procedures for considering complaints received from data subjects and investigating breaches of national legislation. The first workshop was hosted by the UK Commissioner in Manchester in February of this year. Each authority had selected delegates for the workshop from staff who are directly involved in complaints handling, this meant the discussions were conducted at a practical level.

The workshop, held over two days, was attended by 14 countries, together with a representation from the European Commission. Discussion on the first day centred on each country's approach to domestic complaints handling. The second day was dedicated to a discussion on how to approach the handling of complaints where investigation requires co-operation between national authorities.

A suggested common approach was compiled and a list of areas which require further research and discussion were highlighted for future meetings. The overall conclusion of the workshop was that although there are some areas of potential conflict, there are many common factors in the different approaches which can be built upon to provide a platform for future co-operation.

INTERNATIONAL CYBERCRIME

New computer technologies offer unprecedented opportunities for global communication. Their exploitation by high-tech criminals poses an ever-greater threat to public safety. National laws apply to the Internet and other global networks, and it is evident that these should appropriately criminalise the improper use of computer networks. However, while the enactment and enforcement of criminal laws have been, and remain, a national responsibility, the nature of modern communications networks makes it impossible for any country acting alone to address this emerging high-tech problem. Consequently, there have been moves to develop a common international approach to address the problems thrown up by 'cybercrime'.

Last year the 'Working Party on Police', a sub-committee of the annual European Data Protection Commissioners' Conference, asked our office to write a report on the data protection issues arising from various international initiatives to combat cybercrime. We submitted our completed report to the recent Commissioners' Conference in Stockholm.

Two prominent and related initiatives to combat international cybercrime are being developed by committees of experts under the auspices of the G8 group of nations and the Council of Europe. Of central interest from the point of view of data protection supervisory authorities are proposals being considered by these groups that would compel Internet Service Providers (ISPs), and similar operators, to preserve e-mail communications and traffic data for law enforcement purposes. The logic behind seeking the preservation of such data is that evidence in electronic databases is particularly vulnerable to being deleted at short notice, either if a suspect becomes aware that he is under investigation or because data relating to e-mail are subject to short retention periods.

It is proposed that law enforcement should be able to issue 'orders' or 'notices' requiring that ISPs preserve personal data associated with electronic communications. This would be acceptable provided that strict conditions were laid down in national law prescribing the specific circumstances in which an order or notice could be issued. Conditions should include rules for the period of retention of the data and their destruction if no further authority were given for their retention. Orders and notices should be exceptional procedures necessary to preserve data so that formal authority can be obtained to seize the data, usually by judicial warrant.

Of central concern from a data protection point of view is the proposal being discussed by the G8 and Council of Europe groups, and being sponsored in the wider law enforcement community, that traffic data associated with electronic communications should be routinely preserved for law enforcement purposes. The Working Party on Police recognises that some Member States have already provided by law for automatic retention of this class of data for a short period which might be acceptable as a practical necessity subject to strict conditions restricting access to and use of the data. Nevertheless, it is the view of the Working Party on Police that the routine long-term preservation of data by ISPs for law enforcement purposes would be disproportionate general surveillance of communications and consequently incompatible with Article 8(2) of the European Convention on Human Rights and is also likely to be incompatible with the EU Data Protection Directives. This view was confirmed by European Commissioners at their Stockholm Conference.

In 1995, a Council Resolution was passed on the lawful interception of communications. It set out a number of 'Requirements', based on the needs of law enforcement agencies, which would place a series of obligations on telecoms providers. In November 1998, a draft Council Resolution was produced outlining how the 'Requirements' could be extended to the 'new' technologies (satellite phones, Internet). Under 'ENFOPOL 98', ISPs would have to provide high security 'interception interfaces' on their premises, giving 'real time, full time' access to all their traffic. ISPs would have to provide law enforcement agencies with the names, postal addresses, phone numbers, e-mail addresses, credit card details, PINs and passwords of targets.

In December 1998, 'ENFOPOL 98 Version 2' was produced, a much shorter document than the original. It was seemingly agreed that the existing text setting out the 'Requirements' could be interpreted to cover the new technologies. In March 1999, a third draft was drawn up. 'ENFOPOL 19' differed little from the previous document, incorporating a small number of amendments. The most notable of these stated that with the new technologies the interception interface may be 'virtual' within the network, allowing for remote control. When this draft came before the JHA Council of Ministers in May 1999, it was decided to delay the whole process for further review. Strong criticisms had been made of the proposals by network providers. They centred on the lack of clarity in the proposals and the cost implications. We understand that the draft Resolution is currently being redrafted.

The requirement of the 'ENFOPOL plan' for the installation of an interception infrastructure would be acceptable provided that the means of interception remained under the control of ISPs or other communications providers so that there could be effective judicial intervention to authorise or prohibit interception by law enforcement authorities. In our report we argued that the ENFOPOL Plan should be redrafted in a restrictive manner to achieve that end.

European Data Protection Commissioners agreed at the Stockholm Conference to affirm the conclusions of the Working Party on Police as set out in our report. The Commissioners agreed to raise these matters with national governments in such manner as they consider appropriate.

CASE STUDY

Unlawful procurement

A man and his girlfriend attempted to unlawfully procure financial information, concerning his ex-wife, from his ex-wife's bankers. The bank was suspicious of the enquiry and made no disclosure. Following investigation the man and his girlfriend were both fined.

OECD

We have continued to support the work of OECD in carrying forward the Declaration on the Protection of Privacy on Global Networks adopted by Ministers at Ottawa in October 1998. The Deputy Commissioner has worked closely with the OECD Secretariat and has attended as part of the DTI - lead delegation the meetings of the Working Party on Information Security and Privacy. We have also had the opportunity this year both to help OECD and broaden the experience of a member of our staff by seconding a Compliance Manager to work with the Secretariat in Paris for two months. While in Paris our staff member was able to contribute to the final work on one of the most useful of the current OECD privacy projects, namely the Privacy Policy Statement Generator. This tool which is both educational and practical has already in its development versions proved valuable to those developing privacy statements for websites. We look forward to the public release of the Generator and congratulate not only the OECD Secretariat but also Daimler-Chrysler and Microsoft who contributed to the work for this valuable initiative. We also note the forthcoming report on contractual solutions to Transborder Dataflow problems which we hope will prove to be a helpful study of what can be achieved by contractual means to protect personal privacy. Finally, in connection with OECD, we look forward to the future work on privacy and data protection and particularly to the Conference on Alternative Dispute Resolution in the autumn of 2000 which is another practical initiative to secure the position of individuals in E-Commerce and thereby strengthen confidence in global networks.

EUROPEAN POLICE OFFICE (EUROPOL)

We have been designated as the national supervisory body as required by the Europol Convention, as a result of which we are required to carry out regular data protection audits of the UK's participation in the Europol project. Europol commenced work in July 1999 and in order to ensure that the Act was being complied with from the beginning, we used the draft data protection compliance audit (referred to in Chapter 7) to carry out an audit in November of last year. We are pleased to report that the audit did not reveal any significant data protection concerns and that the activities of the UK's Europol Liaison Officers were in accordance with the data protection safeguards contained in the Europol Convention.

financial matters

FINANCIAL POSITION TO 31 MARCH 2000

Year ended 31 March	Office Expenditure	Other Expenditure (note 1)	Receipts (note 2)	Cumulative Financial Position In Cash Terms	Cumulative Financial Position In Accruals Terms (note 3)	Accrued Fees (note 4)
£'000	£'000	£'000	£'000	£'000	£'000	£'000
1985	308	31	-	(339)		
1986	1,696	58	424	(1,669)		
1987	2,422	72	2,757	(1,406)		
1988	2,650	60	930	(3,186)		
1989	2,624	60	1,294	(4,576)		
1990	2,975	67	5,428	(2,190)		
1991	3,153	83	2,068	(3,358)		
1992	3,402	95	2,425	(4,430)	(9,191)	1,503
1993	3,723	78	7,842	(389)	(9,469)	5,903
1994	3,449	83	4,494	573	(7,913)	5,519
1995	3,798	69	3,420	126	(6,417)	3,673
1996	3,975	64	7,072	3,159	(5,526)	5,752
1997	4,025	65	5,173	4,242	(4,471)	5,697
1998	3,660	79	4,913	5,416	(2,527)	4,864
1999	4,190	82	7,586	8,730	(830)	6,538
2000	4,713	94	5,477	9,400	601	9,131
Totals to 31 March 2000	50,763	1,140	61,303	9,400	601	9,131

Notes:

1. 'Other expenditure' includes that incurred in respect of the Data Protection Commissioner (Registrar), the Data Protection Tribunal and related Home Office costs.

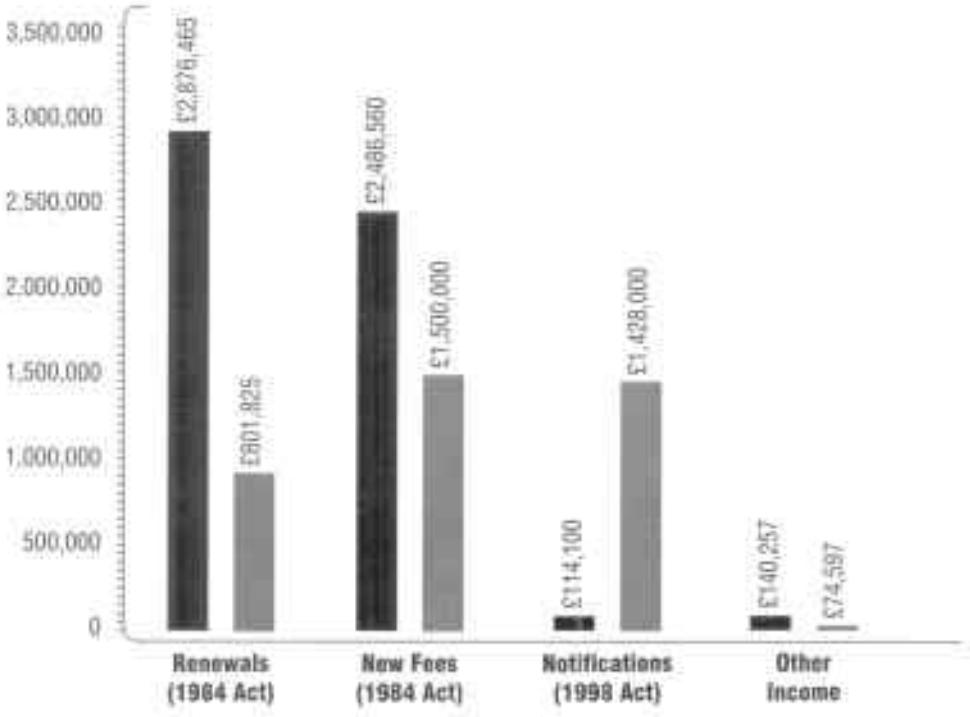
2. 'Receipts' include registration fees and other receipts such as interest on unallocated grant-in-aid in hand invested at overnight rates.

3. From 1992 onwards, the cumulative position under accruals accounting principles is given, adopting a 'full cost' approach. From 1985 these figures incorporate notional costs and are also subject to the Treasury 'GDP deflator'.

4. Under the accruals method of accounting, fees received have been spread over the three year registration period, thus providing an 'accrued fees' figure to be carried forward to future years.

Analysis of actual and forecast income 1999/2000

(in cash terms)



A full statement of account can be found in the Account

Analysis of actual and forecast income 2000/2001

(in cash terms)

	£
notifications – new 88.7%	1,680,000
notification – new 6.0%	114,100
other income 5.3%	100,000
TOTAL	1,894,100

How the grant was spent 1999/2000

(in cash terms)

	£
staff costs 49%	2,295,763
IT support 17.5%	821,740
other running costs 4.4%	206,387
accommodation 10.8%	503,985
education and awareness 11.4%	536,235
VAT 6.7%	316,178
carried forward 0.1%	6,360
TOTAL	4,686,648

Our spending plans for 2000/2001

(in cash terms)

	£
staff costs 45.7%	2,209,915
IT support 13.4%	648,500
other running costs 4.5%	215,770
accommodation 9.7%	467,240
education and awareness 19.4%	935,700
VAT 7.4%	357,235
TOTAL	4,834,360

the year ahead

With the new Office reorganisation in prospect, we have grouped our objectives for the year under each of the four main aims. A number of objectives are extracted below. Our business plan includes the full set of objectives for the year.

OUR OVERARCHING AIM IS:

To ensure that the statutory duties placed upon us are met, efficiently and effectively. To do this we aim to be an organisation responsive to change and ready to manage risk in a way which will allow the resources available to us to be best used.

Objectives:

Agree a plan to achieve the most appropriate structure to best implement our new responsibilities, with its staffing and related needs.

Complete the transition from 1984 Act to 1998 Act operations, ensuring that procedures are in place to deal with all revised operational functions and that those procedures are reviewed in the light of early experience.

Develop systems for effective monitoring of performance in respect of all operational functions and to establish baseline measures.

AIM:

Ensure that policy makers give appropriate weight to individuals' rights.

Objectives:

Seek to ensure by the development of standards, codes, certification programmes and other co-regulatory methods that e-commerce players implement data protection on electronic networks and in particular by end of 2000 to develop and publish design notes for system developers to ensure that privacy protection is incorporated in standard design methodologies.

Participate in European and international activities directed towards the effective implementation of privacy protection by legislative or co-regulatory means.

Organise a further meeting of the EU Data Protection Commissioner's Police etc. Working Party by the end of 2000, and participate in other working groups.

Follow progress of the Freedom of Information Bill, giving advice where appropriate, and develop plans for establishing the Information Commissioner's functions following Royal Assent.

AIM:

Ensure those who handle information both in the public sector and in the private sector are aware of their obligations and act accordingly.

Objectives:

Review existing data protection guidance published by the Office. Prepare and commence implementation of a programme for the phased revision and re-publishing of guidance under the Data Protection Act 1998.

Issue a code of practice on the use of CCTV in public places.

Develop and publish a code of practice on the use of personal data in employment under the Data Protection Act 1998.

Finalise and publish the Data Protection Audit Manual.

Promote two mini-conferences/seminars for the Commissioner, on data protection and Freedom of Information.

AIM:

Ensure individuals are aware of their rights to information, and feel confident that those rights are respected and can be exercised.

Objectives:

Implement a national advertising campaign in August/September 2000.

Finalise and launch education packs for primary and secondary schools.

the data protection commissioner account 1999/2000

FOREWORD

Introduction

This Account has been prepared in a form directed by the Secretary of State for the Home Office as set out in the Accounts Direction which is reproduced in Appendix A.

Under paragraph 10(2) of schedule 2 to the Data Protection Act 1998 the Comptroller and Auditor General is appointed auditor to the Data Protection Commissioner.

History

Following implementation of the Data Protection Act 1998 (The Act), on 1st March 2000 the corporation sole by the name of Data Protection Registrar established by the Data Protection Act 1984 continued in existence by the name of Data Protection Commissioner.

Principal Activities

The purposes of the Data Protection Act 1998 are to:

- make the nature and use of personal data in computer systems open to public scrutiny (through promoting and enforcing the Data Protection Principles); and
- ensure good practice in the use, processing and protection of personal data in computer systems (through promoting and enforcing the data protection principles); and
- allow individuals to claim compensation for damage and any associated distress arising from lack of security surrounding personal data which concern them and from inaccuracies in such data.

The above were also the purposes of the Data Protection Act 1984.

The Office is not a typical Non-Departmental Public Body. Such bodies usually have a relationship with Ministers which is based on the delegation of Ministerial powers. The Commissioner is an independent body created by statute who reports directly to Parliament. She is required to carry out those functions laid down in the Act, using only those powers which the Act sets out. All her decisions are subject to the supervision of the Courts and the Data Protection Tribunal.

The Commissioner is responsible for setting the priorities for her office, for deciding how they should be achieved, and is required annually to lay before each House of Parliament a general report on performance.

The Commissioner also has responsibilities in relation to consumer credit, access to personal files, the Telecommunications Directive and Europol.

Fuller details of the Commissioner's activities, and progress on her objectives during the year, are given elsewhere in the annual report.

Results for the Period

The results for the year are set out on pages 82 to 94.

The Office of the Data Protection Commissioner has been financed by a grant-in-aid from the Home Office Vote (Class IV Vote 1 Section G).

Fees

Schedule 2, paragraph 9(1) of the Data Protection Act 1998 provides that all fees and other sums received by the Commissioner in the exercise of her functions under the Act or section 159 of the Consumer Credit Act 1974 shall be paid by her to the Secretary of State.

Prior to 1 March 2000, all monies received by the Registrar in furtherance of her duties under the Data Protection Act 1984 were remitted to the Home Office as appropriations-in-aid, following a Treasury minute of 1986, produced under section 2(3) of the Public Accounts and Charges Act 1891, which changed the arrangement of surrendering receipts to the Consolidated Fund as provided under paragraph 6(1) of the Act.

Charitable Donations

No charitable donations were made in the year ended 31 March 2000.

Change to Accruals Accounts

This is the first year of preparing the account on an accruals basis and the changeover has had an important impact on the financial statements of the Data Protection Commissioner with the creation of a balance sheet and the identification of fixed assets valued at £65,236.

Year 2000 Issues

There was no significant disruption arising from Year 2000 issues. During the year £18,340 was spent testing IT systems and no further expenditure is anticipated in respect of this risk.

Post Balance Sheet Events

There are no significant events to report.

Compliance with Public Sector Payment Policy

The Office has adopted a policy on prompt payment of invoices which complies with the 'Better Payment Practice Code' as recommended by Government. In the year ending 31 March 2000, 84% (1998/99 – 94%) of invoices were paid within 30 days of receipt or in the case of disputed invoices, within 30 days of the settlement of the dispute.

The reduction in performance arose in the first few months of the year as a result of staffing difficulties. In the period since September 1999 the percentage of invoices paid promptly was 96%.

The target percentage was 95%.

Employee Policies

The Commissioner's Equal Opportunities policy aims to ensure that no potential or actual employee receives more or less favourable treatment on the grounds of race, colour, ethnic or national origin, marital status, sex, sexual orientation, disability or religious belief. An Employment Service Disability Advisor has commented on the Commissioner's "positive attitude and commitment" in the employment of people with disabilities.

The Commissioner is committed to obtaining accreditation under Investors in People and as such places importance on ensuring priority is given to the provision of appropriate training to enable staff to develop skills and understanding of their roles in line with the aims and objectives of the Office.

Future Developments

The Commissioner will continue to monitor the Freedom of Information Bill currently before Parliament, and take account of the responsibilities it may confer upon her.

Elizabeth France

Elizabeth France
The Data Protection Commissioner
June 2000

statement of the data protection commissioner's responsibilities

Under paragraph 10(1)(b) of schedule 2 to the Data Protection Act 1998 the Commissioner is required to prepare a statement in respect of each financial year a statement of account in such form as the Secretary of State may direct. The accounts are prepared on an accruals basis and must give a true and fair view of the Data Protection Commissioner's state of affairs at the year end and of her income and expenditure, total recognised gains and losses and cash flows for the financial year.

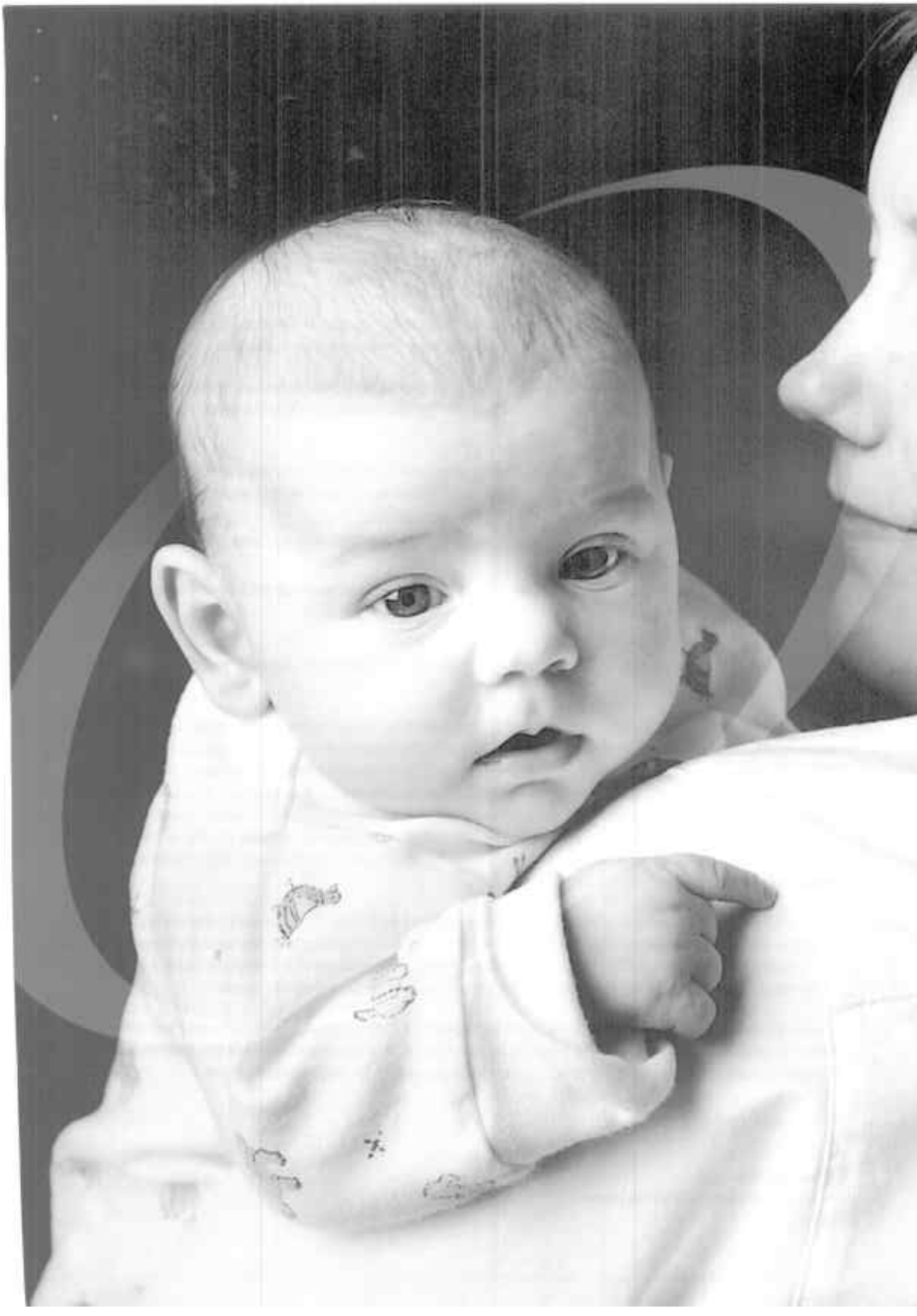
In preparing the accounts the Commissioner is required to:

- observe the Accounts Direction issued by the Secretary of State with the approval of the Treasury, including the relevant accounting and disclosure requirements, and apply suitable accounting policies on a consistent basis;
- make judgements and estimates on a reasonable basis;
- state whether applicable accounting standards have been followed, and disclose and explain any material departures in the financial statements;
- prepare the financial statements on the going concern basis, unless it is inappropriate to presume that the Office of the Data Protection Commissioner will continue in operation.

As the senior full-time official, the Commissioner carries the responsibilities of an Accounting Officer. Her relevant responsibilities as Accounting Officer, including her responsibility for the propriety and regularity of the public finances and for the keeping of proper records, are set out in the Non-Departmental Public Bodies' Accounting Officer Memorandum, issued by the Treasury and published in Government Accounting.

Elizabeth France

Elizabeth France
The Data Protection Commissioner
June 2000



statement on the system of internal financial control

As Accounting Officer, I acknowledge my responsibility for ensuring that an effective system of internal financial control is maintained and operated by the Office of the Data Protection Commissioner.

The system can provide only reasonable and not absolute assurance that assets are safeguarded, transactions authorised and properly recorded, and material errors or irregularities are either prevented or would be detected within a timely period.

The system of internal financial control is based on a framework of regular management information, administrative procedures including the segregation of duties, and a system of delegation and accountability. In particular, it includes:

- comprehensive budgeting systems with an annual budget which is reviewed and agreed by a meeting of the corporate management members;
- regular reviews by the senior management of periodic and annual financial reports which indicate financial performance against the forecasts;
- setting targets to measure financial and other performance;
- a system of delegated authority in respect of commitment to spend and actual expenditure which provides overall control assurance.

Internal audit of the Office of the Data Protection Commissioner is conducted on its behalf by the Home Office Audit and Assurance Unit (AAU) which operates to standards defined in the Government Internal Audit Manual. The work of the AAU is informed by an analysis of the risk to which the Office of the Data Protection Commissioner is exposed, and annual internal audit plans are based on this analysis. The analysis of risk and the internal audit plans are endorsed by the Office of the Data Protection Commissioners Audit Committee and approved by me. At least annually AAU provides me with a report on internal audit activity in the Office. The report includes the AAU's independent opinion on the adequacy and effectiveness of the Office's systems reviewed during the year.

My review of the effectiveness of the system of internal financial control is informed by the work of the internal auditors, the Audit Committee which overseas the work of the internal auditors, the executive managers within the Office who have responsibility for the development and maintenance of the financial control framework, and comments made by the external auditors in their management letter and other reports.

As Accounting Officer, I am aware of the recommendations of the Turnbull Committee and I am taking reasonable steps to comply with the Treasury's requirement for a statement of internal control to be prepared for the year ended 31 March 2002, in accordance with guidance [to be] issued by them.

Elizabeth France

Elizabeth France
The Data Protection Commissioner
June 2000

the certificate and report of the comptroller and auditor general to the houses of parliament

I certify that I have audited the financial statements on pages 82 to 94 under the Data Protection Act 1998. These financial statements have been prepared under the historical cost convention as modified by the revaluation of certain fixed assets and the accounting policies set out on pages 86 and 87.

Respective responsibilities of the Data Protection Commissioner and Auditor

As described on page 76, the Data Protection Commissioner is responsible for the preparation of the financial statements and for ensuring the regularity of financial transactions. The Commissioner is also responsible for the preparation of the other contents of the Annual Report. My responsibilities, as independent auditor, are established by statute and guided by the Auditing Practices Board and the auditing profession's ethical guidance.

I report my opinion as to whether the financial statements give a true and fair view and are properly prepared in accordance with the Data Protection Act 1998 and directions made thereunder by the Secretary of State, and whether in all material respects the income and expenditure have been applied to the purposes intended by Parliament and the financial transactions conform to the authorities which govern them. I also report if, in my opinion, the Foreword is not consistent with the financial statements, if the Commissioner has not kept proper accounting records, or if I have not received all the information and explanations I require for my audit.

I read the other information contained in the Annual Report and consider whether it is consistent with the audited financial statements. I consider the implications for my certificate if I become aware of any apparent mis-statements or material inconsistencies with the financial statements.

I review whether the statement on page 78 reflects the Commissioner's compliance with Treasury's guidance 'Corporate governance: statement on the system of internal financial control'. I report if it does not meet the requirements specified by Treasury, or if the statement is misleading or inconsistent with other information I am aware of from my audit of the financial statements.

Basis of Opinion

I conducted my audit in accordance with Auditing Standards issued by the Auditing Practices Board. An audit includes examination, on a test basis, of evidence relevant to the amounts, disclosures and regularity of financial transactions included in the financial statements. It also includes an assessment of the significant estimates and judgements made by the Data Protection Commissioner in the preparation of the financial statements, and of whether the accounting policies are appropriate to the Commissioner's circumstances, consistently applied and adequately disclosed.

I planned and performed my audit so as to obtain all the information and explanations which I considered necessary in order to provide me with sufficient evidence to give reasonable assurance that the financial statements are free from material mis-statement, whether caused by error, or by fraud or other irregularity and that, in all material respects, the income and expenditure have been applied to the purposes intended by Parliament and the financial transactions conform to the authorities which govern them. In forming my opinion I have also evaluated the overall adequacy of the presentation of information in the financial statements.

Opinion

In my opinion:

- the financial statements give a true and fair view of the state of affairs of the Data Protection Commissioner at 31 March 2000 and of the income and expenditure, total recognised gains and losses and cash flows for the year then ended and have been properly prepared in accordance with the Data Protection Act 1998 and directions made thereunder by the Secretary of State; and

- in all material respects the income and expenditure have been applied to the purposes intended by Parliament and the financial transactions conform to the authorities which govern them.

I have no observations to make on these financial statements.

John Bourn

John Bourn
Comptroller and Auditor General
23 June 2000

National Audit Office
157 - 197 Buckingham Palace Road
Victoria
London SW1W 9SP

income and expenditure account for the year ended 31 march 2000

	Note	1999/2000 £	1999/2000 £	1998/1999 £	1998/1999 £
Income					
Grant-in-aid	2	4,694,240		4,216,355	
Other Income	6	84,220		83,880	
			4,778,460		4,300,235
Expenditure					
Staff Costs	5	2,028,953		1,968,850	
Other Operating Costs	7	2,675,107		2,270,895	
Depreciation of Tangible Fixed Assets	8	17,606		21,355	
			(4,721,666)		(4,261,100)
			56,794		39,135
Operating Surplus					
Fee Income	3		5,837,495		5,762,222
Interest Receivable			56,037		68,172
Notional Cost of Capital			3,250		6,571
Surplus for the year before appropriations			5,953,576		5,876,100
Notional Cost of Capital Reversal			(3,250)		(6,571)
Appropriations due to the Home Office			(5,977,752)		(5,914,274)
Retained Deficit for the year			(27,426)		(44,745)

STATEMENT OF TOTAL RECOGNISED GAINS AND LOSSES FOR THE YEAR ENDED 31 MARCH 2000

	Note	1999/2000 £	1998/1999 £
Retained Deficit for the year		(27,426)	(44,745)
Unrealised surplus on revaluation of assets	12	3,349	-
Total recognised losses relating to the year		(24,077)	(44,745)

The notes on pages 86 to 94 form part of these accounts

BALANCE SHEET AS AT 31 MARCH 2000

	Note	£	31 March 2000 £	£	31 March 1999 £
Fixed Assets					
Tangible fixed assets	8		55,345		65,236
Current Assets					
Debtors and prepayments	9	9,213,851		9,571,249	
Cash at bank and in hand	14	77,555		246,067	
		9,291,406		9,817,316	
Creditors (amounts falling due within one year)	10	(5,230,531)		(5,148,983)	
Net Current Assets			4,060,875		4,668,333
Creditors (amounts falling due after one year)	11		(4,078,532)		(4,662,930)
Net Assets			37,688		70,639
Capital and Reserves					
Income and Expenditure Reserve	12		(17,657)		5,403
Other Reserves	12		55,345		65,236
			37,688		70,639

The notes on pages 86 to 94 form part of these accounts

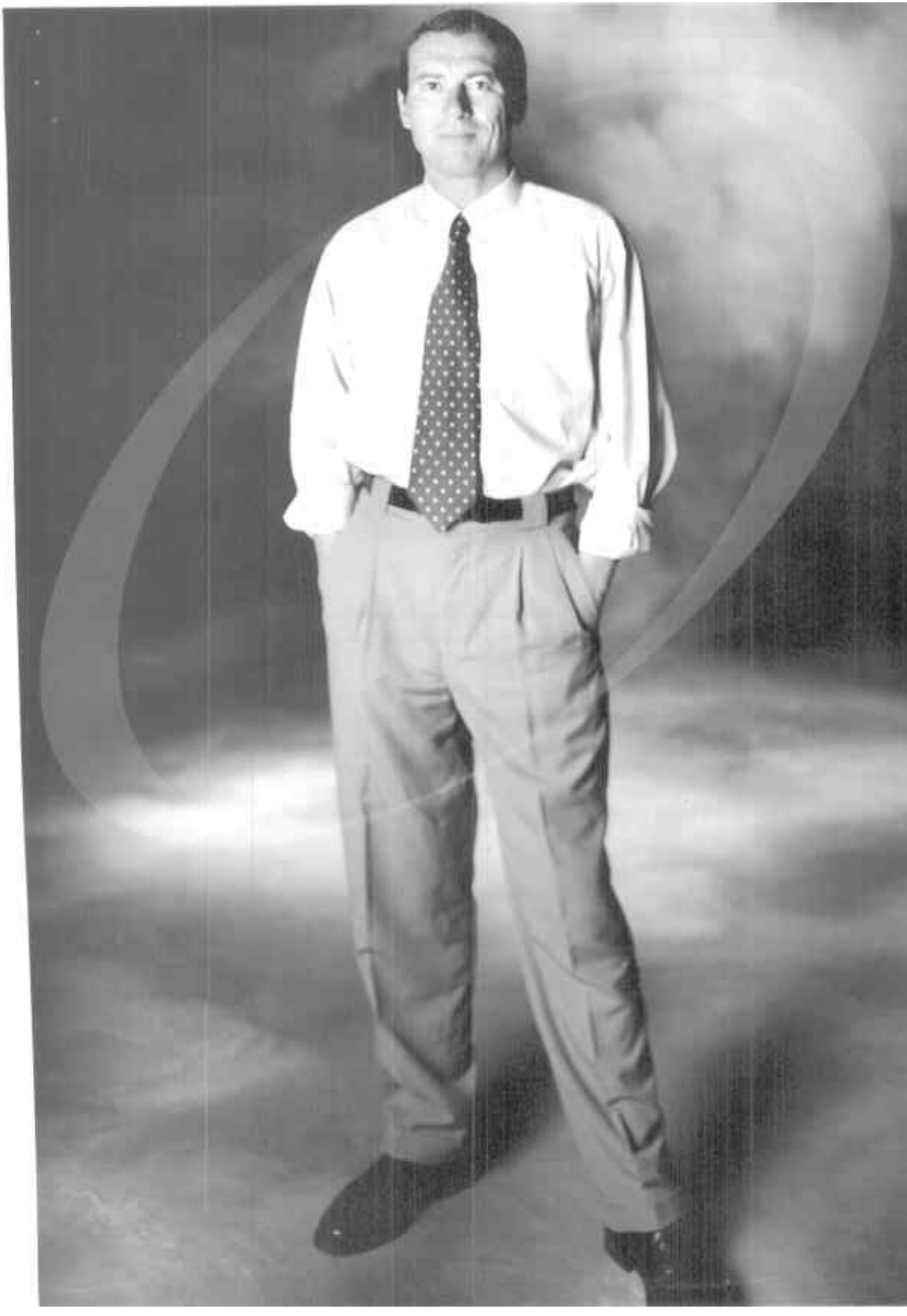
Elizabeth France

Elizabeth France
The Data Protection Commissioner
June 2000

cashflow statement for the year ended 31 march 2000

	Note	1999/2000 £	1999/2000 £	1998/1999 £	1998/1999 £
Net cash inflow from operating activities	13		84,933		87,180
Returns on investments and servicing of finance					
Interest Received			56,037		68,172
Net Cash Outflow before Financing			140,970		155,352
Financing					
Fee Income Received	3	5,477,125		7,434,701	
Less: Income Appropriated to the Home Office	4	(5,786,607)		(7,484,150)	
			(309,482)		(49,449)
(Decrease)/ Increase in cash			(168,512)		105,903

The notes on pages 86 to 94 form part of these accounts



notes to the accounts

1. STATEMENT OF ACCOUNTING POLICIES

1.1 Accounting Convention

This Account has been prepared in a form directed by the Secretary of State for the Home Office. The Accounts Direction is reproduced in Appendix A.

The Account has been prepared under the historical cost convention, as modified by the inclusion of fixed assets at current cost. The Account meets the accounting and disclosure requirements of the Companies Act 1985 and the accounting standards issued or adopted by the Accounting Standards Board to the extent that those requirements are appropriate.

1.2 Prior Year Comparatives

This is the first year for which the Commissioner has prepared accounts on an accruals basis. Comparatives for income and expenditure were audited on a receipts and payments basis.

1.3 Grant-in-Aid

Grant-in-Aid received for revenue expenditure is credited to income in the year to which it relates.

A proportion of the grant-in-aid received, equal to expenditure on fixed asset acquisitions in the period is taken to the Deferred Government Grant Reserve at the end of the financial year. The amount deferred is released back to the Income and Expenditure Account in line with depreciation charged.

1.4 Tangible Fixed Assets

Assets are capitalised as fixed assets if they are intended for use on a continuous basis, and their original purchase cost, on an individual basis, is £2,000 or more. Fixed Assets are valued at net current replacement cost by using the **Price Index Numbers for Current Cost Accounting** published by the Office for National Statistics.

1.5 Depreciation

Depreciation is provided on all fixed assets on a straight-line basis to write off the cost or valuation evenly over the asset's anticipated life. The principal rates adopted are:

Office fixtures	10 years
Office equipment	5-10 years

1.6 Software and Development Costs

Software and system development expenditure on Information Technology systems is written off in the period in which it is incurred.

1.7 Income Recognition

Fee income comprises notification fees in respect of notifications by data-controllers, under the Data Protection Act 1998 (implemented on 1 March 2000) and registration fees in respect of registrations by data-users under the Data Protection Act 1984.

The notification fee is paid in advance for a period of 1 year, up until 29 February 2000 registration fees were paid in advance for a period up to 3 years. A proportion of this income is therefore deferred and released back to the Income and Expenditure Account over the fee period.

Fee income is remitted regularly to the Secretary of State, and thus a prepayment is included within the Account in respect of income appropriated to the Home Office in advance of recognition of the income in the Income and Expenditure Account.

1.8 Notional Charges

In accordance with the Treasury guidance, **Executive Non-Departmental Public Bodies: Annual Reports and Accounts**, a notional charge for the cost of capital employed in the period is included in the Income and Expenditure Account along with an equivalent reversing notional income to finance the charge. The charge for the period is calculated using the Treasury's discount rate of 6% applied to the mean value of capital employed during the period.

1.9 Operating Leases

Payments made under operating leases on Land and Buildings and Equipment are charged to the Income and Expenditure Account as incurred.

1.10 Value Added Tax

The Data Protection Commissioner is only eligible to register for VAT in respect of office accommodation, sub let back to the landlord.

2. GRANT-IN-AID

	1999/2000	1998/1999
	£	£
Grant Received from Class IV Vote 1 (Section G) (1998/99 - Class VII, N)	4,681,000	4,195,000
Release of Deferred Government Grant in respect of depreciation charged	13,240	21,355
	4,694,240	4,216,355

3. FEE INCOME

Fees are received in respect of notification fees (registration fees prior to 1 March 2000) and these monies are paid over to the Home Office who have appropriated it in aid of Class IV Vote 1 (Section G). Receipts in the period were as follows:

	Data Protection Act 1984 (to 29 Feb 2000)	Data Protection Act 1998 (from 1 Mar 2000)	1999/2000	1998/1999
	£	£	£	£
Deferred income at 1 April 1999	9,491,339	–	9,491,339	7,818,860
Cash received for fees	5,363,025	114,100	5,477,125	7,434,701
Deferred income at 31 March 2000	(9,021,623)	(109,346)	(9,130,969)	(9,491,339)
Fee Income from external fees	5,832,741	4,754	5,837,495	5,762,222

4. APPROPRIATIONS

	1999/2000	1998/1999
	£	£
Grant Received for fees (note 3)	5,477,125	7,434,701
Interest receivable	56,037	68,172
Other income	84,220	83,880
Home Office creditor at 1 April 1999	240,420	137,817
Less Home Office creditor at 31 March 2000	(71,195)	(240,420)
	5,786,607	7,484,150

5. SALARIES

The average number of persons employed by the Commissioner during the year were as follows:

	1999/2000 No.	1998/1999 No.
Corporate management	5	5
Senior Staff	6	8
Other Staff	101	103
Occasional Casuals	2	3
	114	119

The aggregate payroll costs of these persons were as follows:

	£	£
Wages and salaries	1,835,935	1,796,461
Social Security costs	124,023	126,513
Pension Costs	68,995	45,876
	2,028,953	1,968,850

The salary and pension entitlements of the Commissioner are paid directly from the Consolidated Fund, thus are not included above.

5. SALARIES (CONTINUED)

The Commissioner and Deputy Commissioner have consented to the disclosure of the salary and pension entitlements below:

	Salary (£'000)	Real increase in pension at 60 (£'000)	Total Accrued Pension at 60 at 31 Mar 2000 (£'000)
Elizabeth France Data Protection Commissioner	65-70	0-2.5	20-25
Francis Aldhouse Deputy Commissioner	55-60	0-2.5	10-15

"Salary" comprises gross salary and any other allowance to the extent that it is subject to UK taxation.

Pension benefits for the Commissioner and members of staff starting in the year are provided through the Principal Civil Service Pension Scheme (PCSPS, pension benefits for the Commissioner's other staff are provided through The Data Protection Registrar's Staff Pension Scheme, which is a by-analogy scheme to the PCSPS). Each scheme provides benefits on a "final salary" basis at a normal retirement age of 60. Benefits accrue at the rate of 1/80th of pensionable salary for each year of service. In addition a lump sump equivalent to 3 years pension is payable on retirement. Members pay contributions of 1.5% of pensionable earnings in respect of widows/widowers/dependents benefits. Pensions increase in line with the Retail Prices Index. On death, pensions are payable to the surviving spouse at a rate of half the member's pension. On death in service, the schemes pay a lump sum benefit of twice the pensionable pay and also provide a service enhancement on computing the widow(er)'s pension. The enhancement depends on length of service and cannot exceed 10 years. Medical retirement is possible in the event of serious ill-health. In this case pensions are brought into payment immediately without actuarial reduction and with service enhanced as for widow(er) pensions.

Agreement has been reached to transfer the staff within The Data Protection Registrar's Pension Scheme into the Principal Civil Service Pension Scheme, and the transfer is expected to be effected within the next financial year.

In anticipation of that change, contributions were paid directly to PCSPS by the Home Office and do not form part of this Account. The total amount of such contributions in the year ended 31 March 2000 was £229,557.

6. OTHER INCOME

	1999/2000 £	1998/99 £
Pension contributions and transfers	14,713	52,702
Legal Fees Recovered	22,712	24,524
Refund of Business Rates following appeal	45,325	–
Other Income	1,470	6,654
	84,220	83,880

7. OTHER OPERATING COSTS

	1999/2000	1998/99
	£	£
Rent and rates	437,176	409,368
Maintenance, cleaning, heating and lighting	67,684	73,777
Office supplies, printing and stationery	83,795	73,943
Carriage and telecommunications	75,685	59,647
Travel, subsistence and hospitality	162,490	148,071
Staff recruitment	19,474	5,400
Specialist assistance	91,693	86,477
Education and awareness	506,386	509,072
Legal costs	65,826	59,033
Staff training, health and safety	16,739	28,356
Computer bureau	818,779	562,906
Vehicle expenses	1,058	990
Audit fee	15,000	7,300
VAT	313,322	246,555
	2,675,107	2,270,895

8. TANGIBLE FIXED ASSETS

	Equipment & Furniture
	£
Cost or Valuation	
At 1 April 1999	115,781
Revaluations in the year	7,715
At 31 March 2000	123,496
Depreciation	
At 1 April 1999	50,545
Revaluations	4,366
Charged in year	13,240
At 31 March 2000	68,151
Net Book Value	
At 31 March 2000	55,345
At 31 March 1999	65,236

9. DEBTORS

	31 March 2000	31 March 1999
	£	£
Fee income prepaid to the Home Office	9,130,969	9,491,339
Other Prepayments	80,117	76,600
Other debtors	2,765	3,310
	9,213,851	9,571,249
Amounts falling due after more than one year included above are:		
Fee income prepaid to the Home Office	4,078,532	4,662,930

10. CREDITORS; AMOUNTS FALLING DUE WITHIN ONE YEAR

	31 March 2000	31 March 1999
	£	£
Trade creditors	58,034	72,854
Payroll	33,865	–
Accruals	15,000	7,300
Home Office creditor	71,195	240,420
Deferred income	5,052,437	4,828,409
	5,230,531	5,148,983

11. CREDITORS; AMOUNTS FALLING DUE AFTER ONE YEAR

	31 March 2000	31 March 1999
	£	£
Deferred income	4,078,532	4,662,930

12. RESERVES

	Income & Expenditure Reserve	Deferred Government Grant Reserve	Revaluation Reserve	Total
	£	£	£	£
Balance at 1 April 1999	5,403	65,236	–	70,639
(Deficit) in year	(27,426)	–	–	(27,426)
Arising on revaluation in the year	–	–	7,715	7,715
Depreciation due to revaluation	4,366	–	(4,366)	–
Release of deferred government grant	–	(13,240)	–	(13,240)
Balance at 31 March 2000	(17,657)	51,996	3,349	37,688

13. RECONCILIATION OF OPERATING SURPLUS TO NET CASH INFLOW FROM OPERATING ACTIVITIES

	1999/2000	1998/1999
	£	£
Operating Surplus for the year	56,794	39,135
Depreciation provided in year	13,240	21,355
Additional depreciation provided due to revaluation	4,366	-
Release of deferred government grant	(13,240)	(21,355)
Increase in debtors relating to operating activities	(2,972)	(1,181)
Increase in creditors relating to operating activities	26,745	49,226
Net cash inflow from operating activities	84,933	87,180

14. CASH AT BANK AND IN HAND

	31 March 2000	31 March 1999
	£	£
Balance at 1 April 1999	246,067	140,164
(Decrease)/Increase in Cash	(168,512)	105,903
Balance at 31 March 2000	77,555	246,067
Commercial banks	77,375	245,735
Cash in hand	180	332
	77,555	246,067

15. COMMITMENTS UNDER OPERATING LEASES

At 31 March 2000 the Data Protection Commissioner was committed to make the following payments during the next year in respect of operating leases expiring:

	Land and Buildings	
	31 March 2000	31 March 1999
	£	£
within one year	325,862	346,706
between two to five years	1,290,824	1,293,980
after five years	3,791,796	4,114,502
	5,408,482	5,755,188

The leases of land and buildings are subject to rent reviews.

16. CONTINGENT LIABILITIES

The Data Protection Commissioner has entered into a contract (which is not an operating lease) for the provision of IT Services. The cost of cancelling the contract at 31 March 2000 would be £192,078 (31 March 1999 - £nil).

17. CAPITAL COMMITMENTS

At 31 March 2000 no capital commitments were contracted for (31 March 1999 - £nil).

18. LOSSES AND SPECIAL PAYMENTS

There were no losses or special payments to report for the year (31 March 1999 - £nil).

19. POST BALANCE SHEET EVENTS

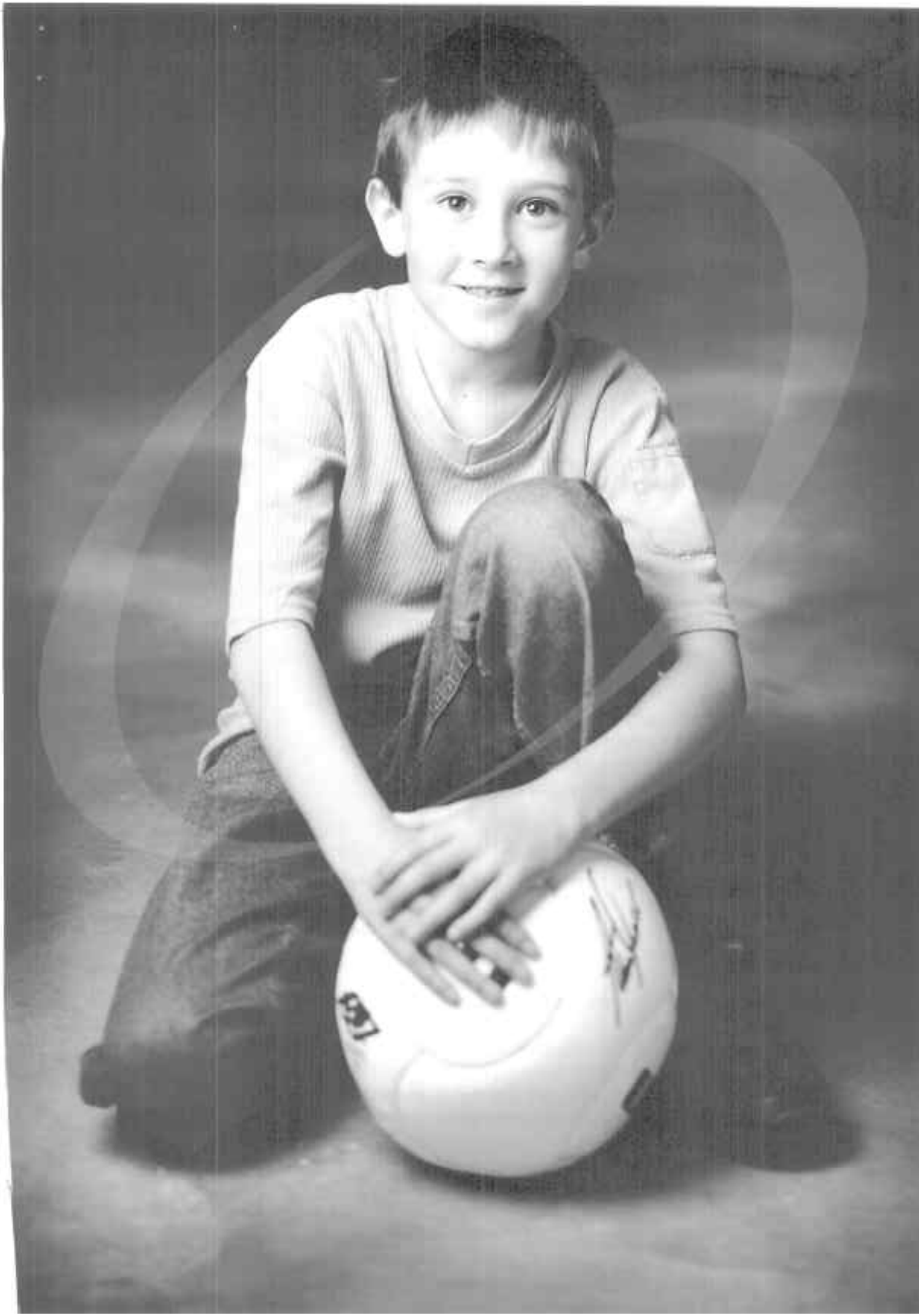
There were no post balance sheet events to report for the year (31 March 1999 - £nil).

20. RELATED PARTY TRANSACTIONS

The Treasury Code of Best Practice for Board members issued in June 1994 recommends that the Chairman and other Board Members should declare any personal interests which may conflict with their responsibilities as Board Members. As the Office of the Data Protection Commissioner has no Board the Treasury has suggested that this recommendation should apply to the Commissioner as Corporation Sole. The Commissioner confirms that she had no personal or business interests which conflict with her responsibilities as Commissioner.

The Home Office is a related party to the Data Protection Commissioner. During the year ending 31 March 2000 no related party transactions, with the exception of the Home Office providing the Commissioner with grant-in-aid, and internal audit services, were entered into. In addition, the Data Protection Commissioner has had various material transactions with other central Government bodies. Most of these transactions have been with the Central Office of Information (COI), Property Advisers to the Civil Estate (PACE) and the Central Computer Telecommunications Agency (CCTA).

None of the key managerial staff or other related parties has undertaken any material transactions with the Data Protection Commissioner during the year.



accounts direction given by the secretary of state for the home department under schedule 5 paragraph (10)(1)(b) of the data protection act 1998, with the approval of the treasury

1. The Data Protection Commissioner shall prepare accounts for the financial year ended 31 March 2000 comprising:

   a) a foreword;
   b) a statement of Accounting Officer's responsibilities;
   c) a statement on the system of internal financial control;
   d) an income and expenditure account;
   e) a statement of total recognised gains and losses;
   f) a balance sheet; and
   g) a cash flow statement.

   including such notes as may be necessary for the purposes referred to in the following paragraphs.

2. The accounts shall give a true and fair view of the income and expenditure and cash flows for the financial year, and the state of affairs as at the end of the financial year.

3. Subject to this requirement, the accounts shall be prepared in accordance with:

   a) generally accepted accountancy practice in the United Kingdom (UK GAAP)
   b) the disclosure and accounting requirements contained in "The Fees and Charges Guide" (in particular those relating to the need for appropriate segmental information for services or forms of service provided) and in other guidance which the Treasury may issue from time to time in respect of accounts which are required to give a true and fair view;
   c) the accounting and disclosure requirements given in "Government Accounting" and in "Executive NDPB's: Annual Reports and Accounts Guidance", as amended or augmented from time to time.

insofar as these are appropriate to the Data Protection Commissioner and are in force for the financial year for which the statement of accounts is to be prepared.

4. Clarification of the application of the accounting and disclosure requirements of the Companies Act and accounting standards is given in Schedule 1 attached. Additional disclosure requirements are set out in Schedule 2 attached.

5. The income and expenditure account and balance sheet shall be prepared under the historical cost convention modified by the inclusion of:

   a) fixed assets at their value to the business by reference to current costs; and
   b) stocks at the lower of net current replacement cost (or historical cost if this is not materially different) and net realisable value.

6. This Accounts Direction shall be reproduced as an appendix to the accounts.

Signed by authority of the Secretary of State for the Home Department.

E A Grant
Head of Liquor, Gambling and Data Protection Unit
Constitutional and Community Policy Directorate
Home Office
20 June 2000

the data protection commissioner

schedule 1

APPLICATION TO THE COMPANIES ACT'S REQUIREMENTS

1. The disclosure exemptions permitted by the Companies Act in force for the financial year for which the statement of accounts is to be prepared shall not apply to the Data Protection Commissioner unless specifically approved by the Treasury.

2. The foreword shall contain the information required by the Companies Act to be disclosed in the Directors' Report, to the extent that such requirements are appropriate to the Data Protection Commissioner.

3. In preparing its income and expenditure account, the Data Protection Commissioner shall adopt format 2 prescribed in Schedule 4 of the Companies Act to the extent that such requirements are appropriate to the Data Protection Commissioner and taking account of the requirements of Schedule 2 to this Direction. This analysis should enable the user of the accounts to gain appreciation of the principle elements of the income and expenditure of the Office of the Data Protection Commissioner.

4. In preparing its balance sheet the Data Protection Commissioner shall adopt format 1 prescribed in Schedule 4 to the Companies Act to the extent that such requirements are appropriate. The Data Protection Commissioner shall also take account of the requirements of Schedule 2 to this Direction. The balance sheet totals shall be struck at total assets less current liabilities:

5. The foreword and balance sheet shall be signed by the Accounting Officer and dated.

6. The Data Protection Commissioner is not required to include a note showing historical cost profits and losses as described in Financial Reporting Standard 3 (FRS 3).

schedule 2

ADDITIONAL DISCLOSURE REQUIREMENTS

1. The foreword shall, inter alia:

   a) state that the accounts have been prepared in a form directed by the Secretary of State with the consent of the Treasury in accordance with paragraph 10(1) of Schedule 5 to the Data Protection Act 1998.
   b) include a brief history of the Office of the Data Protection Commissioner and its statutory background.

a review of the last 15 years of data protection

JUNE 1985

The first report

A year has gone by since the Data Protection Act passed onto the Statute Book. The Registrar's priorities this year include setting up the organisation and the registration process:

- The pilot registration form is launched;
- Guideline One (An introduction and Guide to the Act) becomes available from April 1985 (300k distributed);
- The education and awareness campaign includes distribution of Guidelines and newsletters on the Act.

During the year, we receive over 10,000 telephone and postal enquiries. The first complaints arrive in, totalling 11 in the year.

The Registrar, Eric Howe, states that: "Early priority is to raise the level of understanding and awareness amongst computer users".

"With the very limited effort inevitably available at this stage I have sought to establish a firm foundation for the future".

JUNE 1986

The second annual report

Research carried out this year suggests that awareness of the Act is nearing 100% in large companies. However, nearly 25% of smaller organisations are still not aware of it. A key finding is that a significant number of organisations of all sizes appear to be assuming that the Act doesn't apply to them.

This year sees the publication of information on the Act on Prestel and the production and issue of two booklets detailing frequently asked questions called Questions and Answers (1-20 and 21-34). The Update newsletter is distributed and the office runs two national newspaper advertising campaigns.

The Information line is set up: at the peak of enquiries the office receives 1,200 calls per day. This year the fee for registration is set at £22 for 3 years.

Number of registration applications received	133,000
Registration fee	£22
Number of complaints under the Act received	60
Telephone enquiries handled	65,673

"The positive nature of the Act is apparent. There is wide agreement with the new rights the Act confers on individuals".

JUNE 1987

The third annual report

The Act comes fully into force on 11th November 1987. The Registrar's Investigations department is formed and the first public library version of the register on microfiche is placed in 170 libraries. During the year the volume and substance of complaints increase.

The Office produces a new series of Guidelines and ABTA and the Advertising Association develop Codes of Practice.

The Registrar commissions the first data tracking research on public attitudes towards the use of personal data. The research shows that the public is very supportive of the rights and requirements associated with data protection and privacy. Figures show that 73% of data subjects rate personal privacy as very important and 73% think the Act is very useful, when given a brief description of its provisions. However, the research also shows that 66% of data subjects were not previously aware of the Act.

The Registrar also conducts research on data user's experience of registration and the exemptions given by the Act.

Number of registration applications received	125,000
Registration fee	£22
Number of complaints under the Act received	225
% of data subjects aware of the Act	34%
Telephone enquiries handled	17,000

"Research shows that the public is very supportive of the rights and requirements associated with data protection and privacy."
" Members of the public have to be properly informed of their rights".

Key issues emerging during year:

- *Public Registers;*
- *Proposed Government Data Network;*
- *A possible "National Credit Reference Register";*
- *Disclosure of Information from Police Files.*

JUNE 1988

The fourth annual report

During the year Secondary Legislation modifies the subject access provisions in the Act, particularly regarding health and social work. The registration fee is also increased from £22 to £40 for three years.

The Registrar undertakes discussions with the credit reference agencies.

A rights leaflet "Are you in on the Act?" is produced by the office. Over 1 million copies are circulated as a magazine insertion. This leaflet is also made available through, Citizens' Advice Bureaux, libraries, law centres, consumer advice centres and town hall information points.

The office begins to invest in educating school children and produces a 'Studycard' on data protection for schools.

The Registrar conducts further research on personal privacy. The results show that 66% of data subjects regard personal privacy as very important. However, only 30% are aware of the Act.

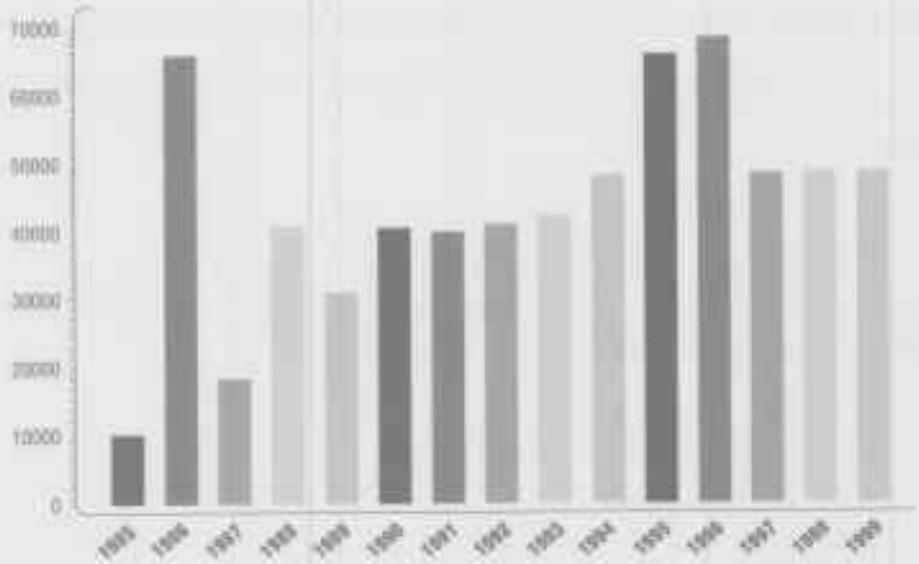
Number of registration applications received	150,000
Registration fee	£40
Number of complaints under the Act received	836
% of data subjects aware of the Act	30%
Telephone enquiries handled	42,000

"Legislation is a creature of its time. It is appropriate therefore, to consider the background against which data protection legislation is set. Research carried out during the year suggests that public concern about personal privacy remains very high. The same research suggests a decline in public confidence in the trustworthiness of many organisations to handle personal information responsibility".

Key issues emerging during the year:

- *Telephone selling;*
- *The Community Charge;*
- *The 1991 Population Census.*

Telephone enquiries



JUNE 1989

The fifth annual report

The Registrar carries out his first prosecutions this year. The Guideline series is updated and a "New Users" card is produced for those who have just purchased or started to use a computer: 6,500 copies are distributed.

Research results show that protecting people's privacy is felt to be important by 72% of data subjects. Awareness of Act amongst data subjects is at 31% and 61% of data subjects rate the Act as useful having been given a brief description of its provisions.

The registration fee is increased from £40 to £56 for three years.

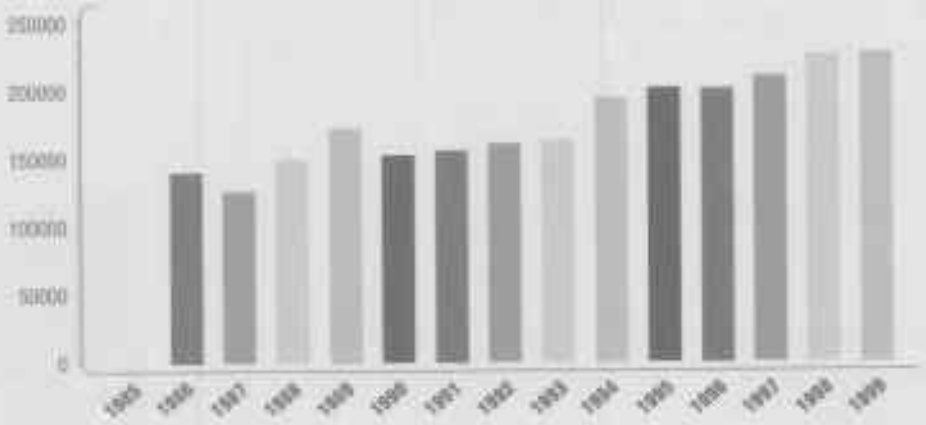
Number of registration applications received	170,000
Registration fee	£56
Number of complaints under the Act received	1,112
% of data subjects aware of the Act	31%
Telephone enquiries handled	31,752
Number of prosecutions	8

"Much of the effort of my office has had to be devoted to work on registration. In looking to the future, I shall be seeking to change the balance of things. More effort and senior skills need to be devoted positively to achieving the more detailed determination and widespread adoption of good data protection practices".

Key issues emerging during the year:

- *The Football Spectators Bill;*
- *Driver information systems;*
- *"Hacking" and the law;*
- *The use of third party information in credit assessment.*

Register entries



JUNE 1990

The sixth annual report

The microfiche copy of the register is withdrawn from public libraries, as it is not widely used. It is replaced by an index to the register, which is published in the form of a book.

A television campaign is launched to raise general awareness of individual's rights and a new rights leaflet, "If there's a mistake on computer about you" is produced.

Research indicates that prompted awareness of Act amongst small organisations is 70% whilst in larger organisations the figure is 95%.

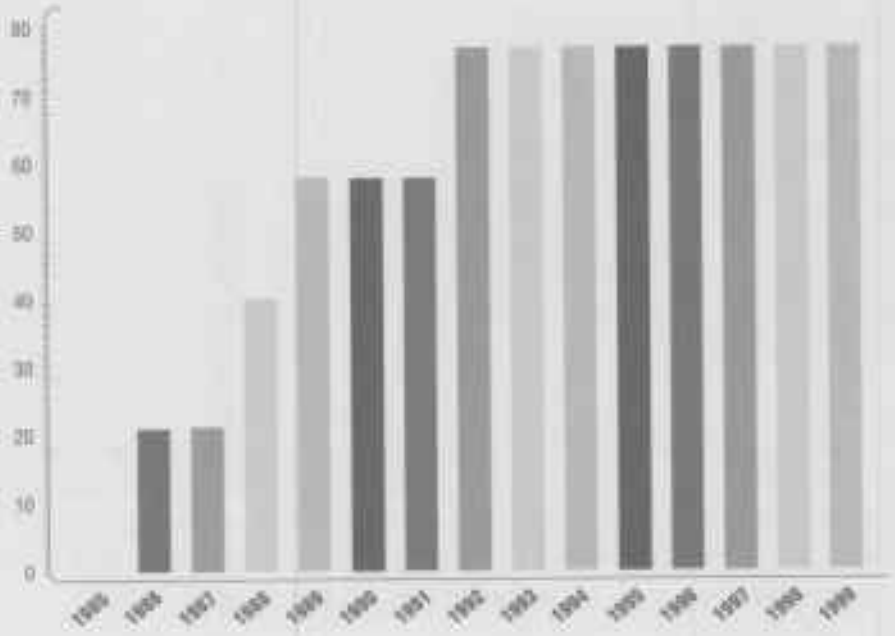
Number of registration applications received	153,000
Registration fee	£56
Number of complaints under the Act received	2,698
% of data subjects aware of the Act	not available
Telephone enquiries handled	41,063
Number of prosecutions	30

"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".

Key issues emerging during the year:

- *The construction and use of personal identification numbers (PINS);*
- *The use of the National Insurance Number;*
- *The Student Loans Scheme;*
- *The National Criminal Records System;*
- *Human Fertilisation and Embryology Bill.*

Registration fee (£)



JUNE 1991

The seventh annual report

The EU draft directive on data protection is published.

The Home Affairs Committee publishes a report on the work of the Office after taking evidence from the Registrar.

The first five hearings and decisions of the Data Protection Tribunal are made. These involved four Community charge registration officers: South Northamptonshire DC, London Borough of Harrow, Rhonda Borough Council, Runnymede Borough Council and one credit reference agency: CCN Credit Systems Limited/CCN Systems Limited.

This year 43,000 copies of the leaflet "If there's a mistake on computer about you" are distributed and 28,000 sets of Guidelines are issued.

A town test is carried out in Cambridge to determine whether there were computer users who had failed to register under the Act. The results of the test indicate that almost 1 in 4 businesses visited should have registered but had not done so.

Research indicates that 70-73% of data subjects rate personal privacy as very important, whilst awareness of the Act amongst data subjects is recorded at 37%.

Research into the use of computers by small organisations indicates a significant rise since 1986: from 31% in 1986 to 45% in 1991. Prompted awareness of the Act amongst small organisations is at 87% and at 95% amongst large organisations.

Number of registration applications received	160,000
Registration fee	£56
Number of complaints under the Act received	2,419
% of data subjects aware of the Act	37%
Telephone enquiries handled	40,445
Number of prosecutions	17

"In my Annual Report in 1987 I discussed data protection as a new public policy takings its steps in a complex society. Perhaps this year will come to be seen as the one in which this infant grew into a fuller role in public and political debate. The first appeals to the Data Protection Tribunal have been heard and determined in this year. I am pleased that the Tribunal, on the arguments heard so far, has upheld the views of the law expressed in the Guideline series published by my office".

Key issues emerging during the year:

- *The New Police National Computer System (PNC);*
- *Co-operation in international policing;*
- *Lifestyle profiling for direct marketing;*
- *The Child Support Bill;*
- *DNA Profile Databases;*
- *Photographs on driving licences;*
- *Document image processing;*

JUNE 1992

The eighth annual report

This year the registration fee increases from £56 to £75 for three years.

The leaflet "What is data protection?" is produced and 40,000 copies distributed. Posters and 'reminder' stickers are produced and distributed to data users.

A small advertising campaign entitled "Ignorance is no defence" runs in business journals and a series of one day seminars are arranged for the advertising & marketing industry.

Research amongst data subjects indicates that 78% rate protecting personal privacy as very important. Awareness of the Act amongst data subjects is 38%.

Data user research indicates that prompted awareness of the Data Protection Act is 88% amongst small organisations and 97% amongst large companies.

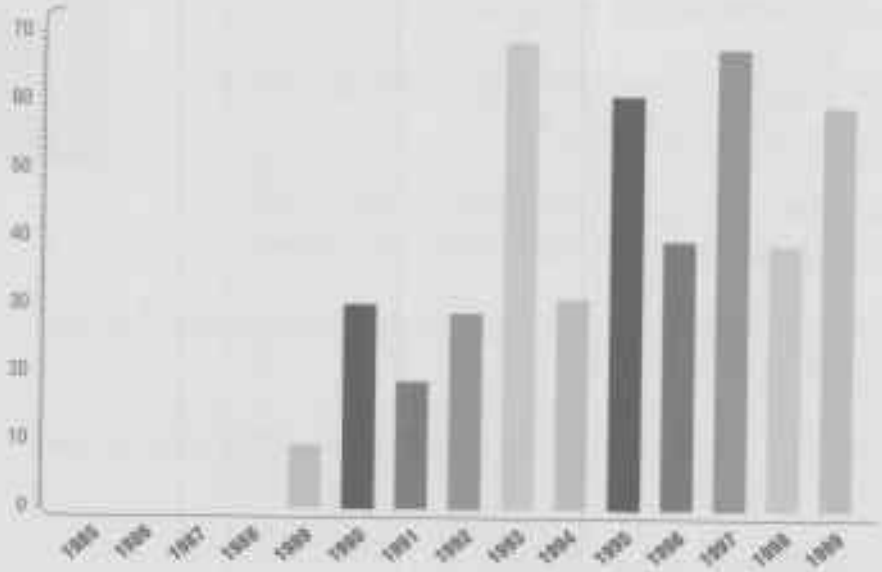
Number of registration applications received	164,500
Registration fee	£75
Number of complaints under the Act received	1,747
% of data subjects aware of the Act	38%
Telephone enquiries handled	42,207
Number of prosecutions	27

→ **"There can be no such thing as absolute individual privacy. Balances need to be struck between the right to privacy and other public objectives. Thus, privacy will be challenged by the need for national security; for financing the nation; for a healthy population; for protection against crime; and by the rights and freedoms of others. The (Council of Europe) Convention recognises this. Without adequate protection there is a grave danger that individual privacy will be whittled away".**

Key issues emerging during the year:

- *European Community Draft Directive on Data Protection;*
- *Warning signals on the Police National Computer;*
- *Access to criminal records by local authorities and employers;*
- *The confidentiality of health information;*
- *Council Tax;*
- *Direct marketing and lifestyle databases;*
- *The population census;*
- *Calling Line Identification systems (telecoms);*
- *Data matching;*

Number of prosecutions



JUNE 1993

The ninth annual report

A television campaign is implemented and runs in the Channel 4, Midlands and North of England regions and on satellite television.

A new information pack "Dealing with the Data Protection Act - A Guide for small businesses" is produced and issued to data users. A 15-minute training video is also produced with over 3,000 copies distributed in the year.

The first series of free introductory seminars are held at venues throughout the UK. Two specialist seminars for the Public Sector and Finance Industry are also held in London.

Data subject research indicates that 66% of individuals rate personal privacy as very important and awareness of Act amongst data subjects when prompted is 38%.

Number of registration applications received	166,327
Registration fee	£75
Number of complaints under the Act received	4,590
% of data subjects aware of the Act	38%
Telephone enquiries handled	43,987
Number of prosecutions	68

"That individuals have concerns seems to be confirmed by the complaints received following a television advertising campaign primarily restricted to the Midlands and North of England and to Scotland. During the campaign, the receipt of complaints by my Office rose from a rate of just under 2,000 a year to a rate close to 29,000 a year".

"The proposed European Community Directive on Data Protection is likely to set the stage for United Kingdom legislation on this subject throughout the late nineties".

Advice on lawfulness in the first and second Data Protection Principles is published.

Key issues emerging during the year:

- *A market in personal data?;*
- *Retention of criminal records;*
- *Enforced access to criminal records;*
- *Automatic fingerprint recognition;*
- *The confidentiality of health information;*
- *The NHS number and NHS administrative registers;*
- *Free insurance offers by banks and building societies;*
- *The Code of Banking Practice;*
- *Information Security Standards.*

JUNE 1994

The tenth annual report

This is last report of the first Data Protection Registrar, Eric Howe who retires.

The Tribunal decision on the appeal by Innovations (Mail Order) Ltd is given.

An advertising campaign is carried out in trade publications and a selection of computer magazines. The free introductory video continues to be distributed with 8,500 copies sent out. A mailing to all public libraries on the rights of data subjects also takes place.

A further series of introductory seminars is arranged.

The UK Data Protection Registrar hosts the XVth International Conference of Data Protection & Privacy Commissioners with the theme "All about people".

Data subject research indicates that 66% of individuals rate personal privacy as very important and awareness of Act amongst data subjects when prompted rises to 47%.

Data user research indicates that 86% of small organisations are aware of the Data Protection Act, whilst awareness amongst large organisations is at 97%.

Number of registration applications received	188,766
Registration fee	£75
Number of complaints under the Act received	2,889
% of data subjects aware of the Act	47%
Telephone enquiries handled	48,207
Number of prosecutions	32

"We are heavily into the problem of balancing conflicting public policies. How does privacy balance against freedom of speech, or the health of the nation, or the prevention of crime, or economic benefit?"

Key issues emerging during the year:

- *National identity cards and identity numbers;*
- *Confidentiality of personal financial data;*
- *Genetic screening;*
- *Open Government;*
- *The holding of sensitive personal data by banks;*
- *Sharing of information in the insurance industry;*
- *Fraud prevention measures in the finance industry;*
- *Teleworking and telecottaging;*
- *Geographic information systems;*
- *Smart cards;*
- *The Internet.*

JUNE 1995

The eleventh annual report

The first report of the new Data Protection Registrar, Elizabeth France.

The Registrar sets up an informal advisory board. A diagnostic review of the office is carried out and a new organisation structure put into place.

A new mission statement and a new brand statement are agreed:

Mission statement: "We shall promote respect for the private lives of individuals and in particular for the privacy of their information by:

- implementing the Data Protection Act 1984;
- influencing national and international thinking on privacy and personal information.

Brand statement: "Using the law to protect your information".

The Criminal Justice & Public Order Act creates three new data protection offences related to the unlawful procuring of information.

A number of conferences on the question of confidentiality and identity cards are arranged. The leaflet, "Your complaint" is issued and the booklet: "Identity Cards: putting you in the picture" is published. This year a revised set of Guidelines and new education pack for schools, "Datawatch" are also produced and issued.

The Office receives over 400 complaints about the Child Support Agency.

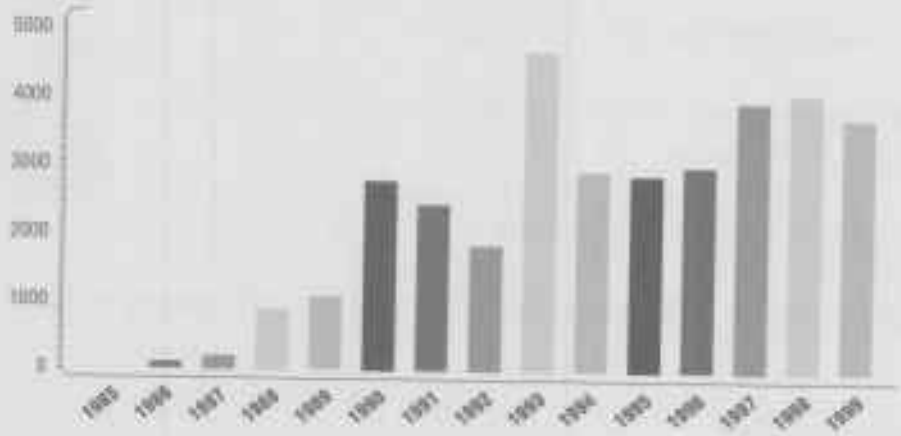
Number of registration applications received	202,476
Registration fee	£75
Number of complaints under the Act received	2,814
% of data subjects aware of the Act	44%
Telephone enquiries handled	65,963
Number of prosecutions	61

→ **"Looking back on changes since 1984 shows the accelerating pace of technological development. The number of users who are able to extract and manipulate data at their desks has increased to an extent which was unimaginable".**

Key issues emerging during the year:

- *Information sharing initiatives in both the public and private sectors;*
- *Local Government reorganisation;*
- *Uses of customer information by regional electricity companies and other utilities.*

Complaints



JUNE 1996

The twelfth annual report

This year sees the formal adoption of the EU General Directive on Data Protection.

"Questions to Answer", a publication concerning the implementation of the Directive in UK law is issued and "Our Answers" our formal response to the Government consultation is published.

Regina v Brown, the first case on the Data Protection Act to reach the House of Lords since the passage of the legislation in 1984 is heard.

The "Privacy at work" conference takes place and a new video training pack is produced.

Research shows that prompted awareness of the Data Protection Act amongst data subjects is at 68%.

Development starts on a new IT System for registration and the complaints handling and compliance advice work of the office are integrated.

Number of registration applications received	201,434
Registration fee	£75
Number of complaints under the Act received	2,950
% of data subjects aware of the Act	48%
Telephone enquiries handled	68,244
Number of prosecutions	39

"Our task must be to educate the next generations of citizens and systems developers to recognise their rights and responsibilities and to understand the power of technology both to erode and enhance the right of each of us to respect for our private lives".

Key issues emerging during the year:

- *Preventing benefit fraud;*
- *Security of health information in the NHS network;*
- *Cryptography;*
- *Electronic Government;*
- *Information superhighway;*
- *Privacy Enhancing Technologies.*

JUNE 1997

The thirteenth annual report

DUIS, the Data User Information System is implemented and the register of data users is published on the Internet.

"Put the record straight" a national television press advertising campaign is rolled out.

A series of seminars are implemented at locations throughout the UK and a conference on "Data Matching" is set up and implemented.

This year also sees the publication of "Our Commitment to You", a leaflet explaining what individuals should expect from the services we provide.

The tracking research on data subject awareness indicates that 72% are aware of the Act or Registrar. The data user study indicates that 89% of small organisations and 98% of larger organisations are aware of the Act or Registrar.

The office is represented at the working party of data protection authorities which is set up under the Directive.

Number of registration applications received	212,943
Registration fee	£75
Number of complaints under the Act received	3,897
% of data subjects aware of the Act	62%
Telephone enquiries handled	47,697
Number of prosecutions	67

"With awareness levels high, and our commitment to keep them high, we can expect to see applications for registration and the number of complaints we receive also remaining at high levels. At the same time we are determined to provide high quality and timely advice to those preparing the Data Protection Bill which will provide our legal framework for the next decade or more. We have a lot to do".

Key issues emerging during the year:

- *Millennium Bomb;*
- *Freedom of Information;*
- *European Convention on Human Rights;*
- *Use of customer information by the privatised utility companies;*
- *Information sharing and data matching;*
- *Access to criminal records for employment vetting.*

JUNE 1998

The fourteenth annual report

The Tribunal Decision on the appeal by British Gas Trading Ltd is published.

Guidance on the use of information by public sector bodies is published in the "Private Lives Public Powers" booklet.

The first of a series of research studies assessing the guidance offered by the Data Protection Registrar is undertaken.

The television campaign, "Put the record straight" is implemented and "Key issues in the community", a week long promotional campaign on a local radio is run. A separate communications campaign targeting GPs and Independent Financial Advisers is implemented.

A further series of seminars are run in conjunction with a commercial supplier.

With the growth in use of the Internet, the Office's website is revised to ensure it is flexible for future development.

Data Subject awareness of the Act and Registrar increases to 73%, whilst awareness amongst small organisations is at 88%, and amongst large business at 97%.

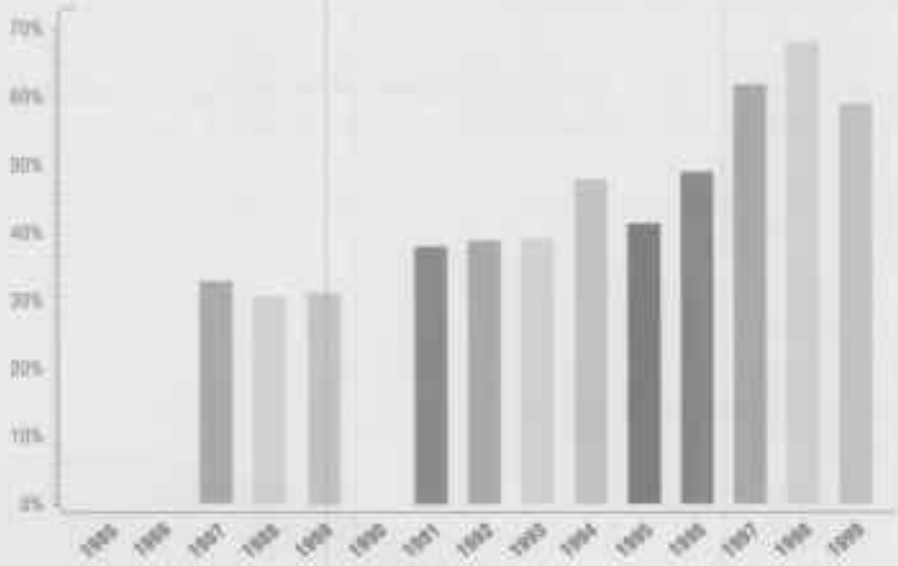
Number of registration applications received	224,909
Registration fee	£75
Number of complaints under the Act received	4,173
% of data subjects aware of the Act	67%
Telephone enquiries handled	48,337
Number of prosecutions	38

"... research indicates that people are concerned about the way that their information is used".

Key issues emerging during the year:

- *Pupil identification numbers;*
- *Loyalty cards;*
- *CCTV;*
- *Genetic testing for insurance purposes;*
- *Unsolicited marketing faxes.*

Awareness of the Act amongst data subjects



JUNE 1999

The fifteenth annual report

Data Protection Act 1998 receives Royal Assent.

Our first guidance on the 1998 Act, "The Data Protection Act 1998 - An Introduction" is published.

The provisions of the Telecommunications Data Protection Directive (97/66/EC) which relate to Direct Marketing come into effect on 1 May 1999.

A workshop involving a range of representatives from consumer groups is run to establish the most effective ways to get the data protection message across to data subjects.

The Tribunal Decision on the appeal by Midlands Electricity plc is published.

A DRTV campaign is run through main Post Offices throughout the UK. Over 200,000 copies of "Using the law to protect your information" are distributed.

A series of seminars on the new law is arranged. The demand for places is high, requiring us to arrange a

further series later in the year.

Number of registration applications received	229,693
Registration fee	£75
Number of complaints under the Act received	3,653
% of data subjects aware of the Act	59%
Telephone enquiries handled	48,549
Number of prosecutions	59

"The last five years have seen a dramatic change in the use of information technology and with this has come an increasing recognition of the risk to personal privacy presented by the processing of personal data".

Key issues emerging during the year:

- *"Modernising Government" proposals;*
- *Release of vehicle keeper information;*
- *Review of electoral procedure and availability of the electoral register;*
- *Use of personal data in employment;*
- *Publication of draft Freedom of Information Bill.*

Printed in the UK for The Stationery Office Limited
On behalf of the Controller of Her Majesty's Stationery Office
Dd5069315. 7/00. 074888. OrdTJ1952

The Office of the Data Protection Commissioner

Wycliffe House

Water Lane

Wilmslow

Cheshire SK9 5AF

To notify call: 01625-545740

Information Line: 01625-545745

Switchboard: 01625-545700

Fax: 01625-524510

DX: 20819 Wilmslow

Website: www.dataprotection.gov.uk

e-mail: mail@dataprotection.gov.uk

Note:

1. The main body of this report outlines the main issues and developments of the office during the sixteenth year of operation of data protection law. Although most figures relate to the year ending 31 March 2000, the report includes references to the developments, which have taken place between the financial year-end and publication.

2. During the year the Data Protection Act 1998 came into force (implemented on 1 March 2000). Where figures relate to responsibilities under the 1984 Act, these may cover a shorter period than in previous years. Where this is the case, the figures are marked and explanatory notes provided.

contents

Annual report and accounts for the year ending 31 March 2000.

The first report of the Data Protection Commissioner on the 16th year of operation of the Data Protection Act 1984.

June 2000.

Presented to Parliament pursuant to Section 52(1) and Schedule 5, paragraph 10(2) of the Data Protection Act 1998.

Ordered by the House of Commons to be printed 11 July 2000.

London: The Stationery Office.

Price £16.50
575

Published by
The Stationery Office Limited
and available from

The Stationery Office
(Mail, telephone and fax orders only)
PO Box 29, Norwich NR3 1GN
General enquiries 0870 600 5522
Order through the Parliamentary Hotline
Lo-Call 0845 7 023474
Fax orders 0870 600 5533
Email book.orders@tso.co.uk
Internet http://www.clicktso.com

The Stationery Office Bookshops
123 Kingsway, London WC2B 6PQ
020 7242 6393 Fax 020 7242 6394
68-69 Bull Street, Birmingham B4 6AD
0121 236 9696 Fax 0121 236 9699
33 Wine Street, Bristol BS1 2BQ
0117 926 4306 Fax 0117 929 4515
9-21 Princess Street, Manchester M60 8AS
0161 834 7201 Fax 0161 833 0634
16 Arthur Street, Belfast BT1 4GD
028 9023 8451 Fax 028 9023 5401
The Stationery Office Oriel Bookshop
18-19 High Street, Cardiff CF1 2BZ
029 2039 5548 Fax 029 2038 4347
71 Lothian Road, Edinburgh EH3 9AZ
0870 606 5566 Fax 0870 606 5588

The Parliamentary Bookshop
12 Bridge Street, Parliament Square
London SW1A 2JX
Telephone orders 020 7219 3890
General enquiries 020 7219 3890
Fax orders 020 7219 3866

Accredited Agents
(See Yellow Pages)
and through good booksellers

ISBN 0-10-556825-2

8224