NINTH REPORT of the Data Protection Registrar June 1993

THE DATA PROTECTION REGISTRAR

LONDON : HMSO

NINTH REPORT

of the

Data Protection Registrar

June 1993

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

Ordered by the House of Commons *to be printed 13 July 1993*

LONDON: HMSO
£13.25 net

736

Contents

APPENDICES

A Personal Note

It seems likely that the European Community (EC) Directive on Data Protection will be finalised late in 1994. After that it can be expected that there will be a two-year run up to a new Data Protection Act. A Registrar coming into post at the beginning of 1994 will have time to bed in and then make his or her own informed contribution to the new legislation.

For this reason, allied to a wish to have more personal time available outside work, I am planning to retire at the end of 1993 rather than at the end of my current term of office in September 1994.

In 1989 I reviewed the Act and reported to Parliament on this. I concluded that the Act should be strengthened for individuals and simplified for computer users. I hold to that view and believe the EC Directive can offer the opportunity to achieve both those objectives. Had the current situation arisen some years ago, I would have welcomed an opportunity to assist data protection in the United Kingdom through its next stage of development.

The present Act has made and continues to make its contribution. It has enabled help to be given to many thousands of individuals who have encountered problems arising from the use of information about them. It has promoted greater openness on the part of computer users and led to helpful privacy-supporting changes and improved practices in both the public and private sectors.

In the private sector significant changes have been made in credit reference and direct marketing activities. In the public sector, legislation has been influenced, for example, to prevent the sale of public records such as the Community Charge Registers. This Report records developments in respect of policing and health activities. In addition, contributions have been made to debates on issues of wide and relevant public interest, such as national identity numbers and identity cards. Annual Reports over the years catalogue a wide variety of activities and a great diversity of issues faced. This one is no exception.

If the next few years are to be interesting ones, they can be no more so than the last nine. The Registrar's job combines what the Banking Services Review Committee termed "unique independence" with a tremendous range of challenges as personal information becomes more widely used and computing ever more pervasive. It has been a privilege to have a job which has been, and continues to be, exciting, rewarding, intellectually stimulating – and greatly enjoyable.

But the Registrar is only one part of the organisation. I started in 1984 with a copy of the Act and a very able secretary. I have been blessed throughout with a superb staff. From the most junior member to the corporate management, they have proved themselves able, hardworking, friendly, loyal and supportive. I noted with pleasure the comment in a recent House of Lords Report that many witnesses remarked on the excellence of my staff.

It would be wrong too not to mention those outside the Office – individuals, computer users and those representing sectoral interests. I have much appreciated how those concerned have been ready to maintain a friendly relationship even on those occasions when my views on the meaning and effect of the Act have been unwelcome.

I was asked by the Home Secretary when taking on the Registrar's job why I wished to do it. My response was that it offered the opportunity to move the world a little. Much of that need for movement remains, for data protection represents a massive long term educational exercise to change the attitudes and practices of a nation.

The next Registrar will not want for interesting tasks and at the appropriate time I will be pleased to wish him or her every success in them. For the moment, for his or her sake – and indeed for that of the country as a whole – I simply hope that the darkening financial cloads prove to herald but a passing storm.

ERIC HOWE

JUNE 1993

1 Introduction

This report is for the year ending 31 May 1993, although in a few cases relevant actions taken since that date have also been included. The layout is sufficiently similar to previous reports to aid those who wish to follow developments over the years. As usual, this year's report ranges widely over activities in both the public and private sectors.

It is some time since I have put general information on the Data Protection Act 1984 in one of these reports. The following brief description may be helpful for new readers.

The Data Protection Act 1984 was the first piece of legislation in the United Kingdom to address the use of computers. It is concerned with information about individuals which is processed by computer (personal data). It introduces significant new rights for individuals to whom that information relates (data subjects). Such an individual generally has the right to:

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

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

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

The Act places obligations on those who control the contents and use of personal data in computers (data users). They must be open about that use through placing details of their activities on a Data Protection Register which is available for public inspection. They must also follow sound and proper practices. These practices are described in eight Data Protection Principles. Amongst other things, the Principles require that personal data should be obtained fairly and be accurate, relevant, not excessive and kept secure. Computer bureaux have more limited obligations mainly concerned with maintaining appropriate security around personal data.

The Data Protection Registrar is appointed by Her Majesty by Letters Patent and reports directly to Parliament. The Registrar is charged with administering the Data Protection Act 1984 and supervising its operation. His decisions are subject to the supervision of the Courts and the Data Protection Tribunal, which is also established by the Act.

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

2 The United Kingdom – A Part of the European Community

It is increasingly necessary, when considering the future position of data protection in the United Kingdom, to have regard to developments in the European Community. These may have fundamental implications for data protection law here, as in the case of the European Community's (EC) Draft Directive on Data Protection. Or, alternatively, they may affect particular United Kingdom activities through specific collaboration between Community members.

I have been pleased to assist in the development of the EC directive through the secondment of one of my staff to work with the Commission in Brussels.

I was also pleased to have the opportunity, along with the Deputy Registrar, to give evidence to the House of Lords Select Committee on The European Communities* which was considering the draft directive. This Committee reported in March 1993.

Following a series of meetings, the Commissioners of Belgium, Denmark, France, Germany, Ireland, Luxembourg, the Netherlands and the United Kingdom have reached common conclusions on the draft directive. The other EC countries had not reached the stage to provide a representative to these meetings. The conclusions have been submitted to the European Commission, the Council of Ministers Working Party and the European Parliament. The common conclusions are given in Appendix 2. They relate closely to the comments which follow. The success of these meetings augurs well for the working party of data protection authorities proposed in the draft directive.

(a) The European Community's Draft Directive on Data Protection

In 1990, the Commission of the European Communities (the Commission) published a package of proposals on data protection including a draft general directive. Following consideration and comment by the European Parliament a revised draft of this directive was published by the Commission in October 1992.

The Commission's initiative is welcome. Establishing rules about the lawfulness of processing, emphasising particularly the consent of the data subject, and the granting of specific rights to individuals would enhance the protection of individuals in the United Kingdom. The revised draft does, however, present a number of practical problems.

A paper with detailed comments was made available by my Office in October 1992. This is reproduced in Appendix 1. It considers whether a European Community directive on data protection is needed. It then describes the principal objectives of the revised draft and picks out some issues for consideration. Finally, it gives more detailed comments on specific articles in the directive before a brief

*The 20th Report (Session 1992-93) from the House of Lords Select Committee on the European Communities, *Protection of Personal Data* (HL Paper 75) published by HMSO.

conclusion. Some of the main points from this paper follow.

(i) *Do we need a European Community Directive on Data Protection?*

A number of European countries have introduced data protection laws to allow them to ratify the Council of Europe Convention on Data Protection (the Convention)*. Ratification by EC Member States has been encouraged by resolutions of the European Parliament, recommendations of the Council of Ministers and Commission initiatives. However, Italy and Greece have still not passed data protection legislation enabling them to ratify the Convention. Italy is actively pursuing legislation and a draft Bill is being considered in Greece.

Even those countries which do have legislation, have legislated in distinctly different ways. The issue of whether one country gives protection equivalent to another has caused some difficulty. There are other practical problems arising from the multi-national nature of some data processing operations. A parent company, which arranges to process the data collected by its various European subsidiaries at a bureau in the United Kingdom, may be quite uncertain which data protection laws it must satisfy and there is always a risk that the requirements of those laws will be inconsistent.

The internal market was established in the European Community at the start of the year. Article 8A of the Treaty of Rome defines the internal market as an area "without internal frontiers in which the free movement of goods, persons, services and capital is ensured in accordance with the provisions of this Treaty". With the advent of the single market, then a single regime for data protection acceptable to all member states would seem to be not only unavoidable but also desirable. Without the free flow of personal data between member states there is a clear danger that the other free movements will be undermined. There would seem, therefore, to be a need for a directive. However, the question remains open as to its particular scope and nature.

(ii) *Principal Objectives of the Revised Draft Directive*

The first objective of the Revised Draft Directive (the revised draft) is to harmonise data protection laws in the Member States. The intention is to harmonise at a high level of protection for individuals and not to prejudice any protection given already by the legislation of individual member states.

The parallel objective of the revised draft is to create an area within which personal data can be transferred without restriction. That is achieved by banning the prohibition or restriction of the flow of personal data between member states on data protection grounds.

(iii) *Some Significant Issues*

The revised draft raises a number of significant issues. Some of these are:

— *A Right to Privacy:* The revised draft emphasises in Article 1(1) that its subject matter is the protection of:

> "The rights and freedoms of natural persons with respect to the processing of personal data, and in particular their right to privacy"

This is a clear, welcome, statement that data protection is a human rights matter rather than any question of the technical regulation of computers. Implementation of the final directive into law here may become a significant element in the debate about the right to privacy in the United Kingdom.

— *Balancing Rights:* Nevertheless, data protection has to be about balancing

* Full references for the drafts of the directive and for the Council of Europe Convention on Data Protection are given in Appendix 1.

rights. A balance has to be struck between those rights contained in Articles 8 and 10 of the European Convention on Human Rights (European Treaty Series No. 5). Article 8 states that everyone has the right to respect for his private and family life, his home and his correspondence. Article 10 states that everyone has the right to freedom of expression.

— *Consent:* The revised draft expressly introduces a requirement for the consent of individuals to the processing of personal data in certain cases. This is particularly so where data are defined as "sensitive", for example, health records. This is a distinct difference from the Act.

There has been considerable comment from organisations representing data users about the impracticability of the consent requirements. It is not true that consent is always required. The revised draft sets out rules which, if followed, should legitimise the collection and processing of personal data in most cases, without the need to gain the consent of the individuals concerned. However, where consent is not obtained, there are additional requirements for data users to inform individuals of the uses and disclosures of information about them.

— *Manual Records:* The revised draft extends data protection to manual records. There has been considerable debate about this and it remains a source of much contention. It is said that no difference in principle can be seen between the risks to individuals created by manual and automated records. On the other hand, the Convention and other international instruments were expressly justified on the basis that the power of automatic processing to assemble, rearrange, manipulate and communicate data posed such a significant potential threat that special legal protection was required to protect the privacy of individuals.

At this stage of the debate, my own view is that some coverage of manual records, related to the sensitivity of the information or its use, might be appropriate. However, a total cover of manual records would seem to be going too far, although a right of access by individuals to such records should be considered.

— *Registration:* A registration system is central to the Act. Registration makes for openness on the part of those processing personal data. It can also be used to regulate undesirable processing. However, a comprehensive scheme of registration carries with it an element of bureaucracy. The inclusion of extensive exemption and simplification procedures will aid concentration on matters of greater, rather than lesser data protection significance. The revised draft seems to allow this. It is important to note, however, that the exemptions from registration contemplated by the revised draft would not release data users from the duty of complying with substantive data protection rules.

— *Subject Access:* The right of an individual to obtain information about him or herself (subject access) is fundamental to data protection objectives. There have to be exemptions such as those permitted by the Convention for national security, defence, criminal investigation and certain other cases, but they have to be restricted to those constituting 'a necessary measure in a democratic society'.

The revised draft gives individuals an important extra right to refuse to exercise their subject access rights under the compulsion of a third party. This is a specific United Kingdom problem, where, for example, prospective employers have required applicants to exercise subject access rights in order to vet their criminal records. The proposal in the revised draft is a step forward but it might be preferable to prohibit a third party

from making such a demand rather than merely granting the right to the individual to resist it.

— *Transborder Data Flow Control:* This issue is complex. Transborder data flow provisions have considerable implications for relations between the EC and non-EC countries. These include those countries which, rather than ratifying the Convention, aim to follow the similar rules in the OECD guidelines, but which do not have private sector data protection legislation on European lines. Most prominent amongst these countries is the United States of America. The Commission has had to try to achieve a protected data protection community whilst not unreasonably disrupting legitimate and important trade links. Providing that positive action is taken to achieve common standards and to tackle problems which arise, the revised draft adds a degree of useful flexibility and is an improvement on the original.

— *Exemption for the Media:* The revised draft contains an article which will compel member states to grant exemptions for the media from data protection laws. The revised article sets the objective of the exemptions as:-

> "to reconcile the right to privacy with rules governing freedom of expression . . ."

The whole article is founded on the footing that there is a right to privacy. It also recognises that the media has a very important role in a democratic society. However, the right to grant exemptions should not be interpreted so widely as to unduly prejudice the protection of privacy which the directive seeks. Issues such as this are particularly relevant at present in the United Kingdom and I return to this subject in Section 3.

— *Fair Obtaining of Information:* The requirement in the Act that information shall be obtained fairly has proved to be of particular practical importance. There have been disputes over the meaning of this requirement with the direct marketing industry. One argument has centred on whether an individual should be informed before the collection of information as to non-obvious uses of it (broadly my view) or can properly be told after collection (a view taken by the industry). Some appeals to the Data Protection Tribunal referred to in Section 6 will assist in resolving the situation.

It is arguable, under the revised draft, whether an individual should be informed before or after information has been obtained from him. It hardly seems adequate to collect information unfairly and then provide the explanation as the revised directive currently might allow. Indeed, that would seem to me to be a reduction in the protection given to individuals by the current United Kingdom legislation.

— *Compensation Rights:* A distinctive benefit for individuals, in both the original and revised drafts, is the wide right to compensation. Under the Act, individuals have rather limited rights to compensation in certain cases of inaccuracy, loss or destruction of data. The proposed directive would extend those rights to compensation to someone "who suffers damage as a result of an unlawful processing or any act incompatible with the national provisions adopted pursuant to the Directive". This extension is welcome but individuals should not thereby be deprived of their existing right to compensation in some cases for distress as well as damage.

— *Implementation Machinery:* The revised draft requires Member States to establish supervisory authorities. There would be some enhancement to the current powers of the Registrar. These will be welcome especially

where they would permit the Registrar to obtain further information in order to exercise his functions and where they would allow information to be obtained about the use of subject access exemptions.

The power under the Act to disseminate information is fundamental to the Registrar's role. Data protection will be most effective when it has become part of the natural thinking of those collecting information and designing systems. Thus they would, as a matter of course, ask themselves whether they have a need for the information, whether it is sufficient and accurate and indeed whether they have satisfied the other data protection principles. This long-term change in attitudes is a major educational task. The functions of supervisory authorities as stated in the revised draft do not expressly include this educative function. It would be a retrograde step if the Registrar were deprived of such powers.

(iv) *Conclusion*

The Data Protection Act introduced measures of protection for individuals which have enabled the United Kingdom to ratify the Council of Europe Convention on Data Protection. However, unlike the Convention, the Act does not refer to privacy, it is simply a statute "to regulate the use of automatically processed information relating to individuals...". On the other hand, the European Community Draft Directive on Data Protection is concerned with privacy and, in its revised form, gives greater control and greater protection to individuals than the Act. It also, helpfully, reduces a bureaucratic burden on data users by allowing simpler registration procedures.

The revised draft is not perfect and there is still room for significant debate, for example, on the cover to be given to manual records and the position of the media. There are also other matters of substance or detail which need to be clarified. Nevertheless, the revised draft is welcome and not generally unreasonable in the broad balance it seeks to set at this stage between individual privacy and other public interests.

A Council of Ministers Working Party is currently considering the revised draft and a directive may finally be in place late in 1994. If this date is achieved, then a new United Kingdom Data Protection Act might be in force around the end of 1996.

(b) Collaborative Activities

Last year I drew attention to moves towards greater co-operation between police and other control authorities in EC member states. It is important that these co-operative ventures develop within an overall framework of data protection control; it is not sufficient to rely solely on national data protection legislation. Specific provisions are needed to reinforce national legislation and some relevant Conventions are being established. A mechanism is also necessary to deal with possible conflicts arising from different national interpretations of those Conventions.

My staff have continued to provide input to the work being led by HM Customs and Excise on a draft Convention for the proposed Customs Information System (CIS). That work has been complicated by the need for member states governments to agree a Council Regulation on Mutual Assistance. This incorporates the provisions of the draft CIS Convention itself with some amendments particularly concerning the role of the European Commission.

One of my senior staff has participated in several meetings during the past year of a drafting group working on data protection provisions for Europol, which covers

co-operation between EC police forces. This has particularly concerned itself with the Europol Drugs Unit. Building on the work of that group, the Home Office is directing further drafting of an overall Convention for Europol. I look forward to being consulted once specific proposals have been formulated. The intelligence role of Europol poses some difficult data protection problems. It is important for a mechanism to be found under which those problems can be solved, if they are not resolved in the Convention itself.

My staff have also attended a meeting of the working group of EC Data Commissioners on policing, customs and related matters.

3 Some Issues in the United Kingdom

In this section I deal with a number of issues with which my Office has been concerned over the last year. The work outlined here is carried out by "policy staff". Unfortunately, in order to cope with the influx of complaints referred to in Section 5, it has been necessary to withdraw a number of staff, if only temporarily, from these activities.

(a) A Market in Personal Data?

During the last year, reports in the Sunday Times have alleged that it is possible to obtain a wide range of information about individuals. Some of the information quoted would appear to derive from confidential sources such as bank accounts and tax records. On the face of it much of the information may be obtained by deception, but illegal actions by members of the staff of computer users cannot be ruled out.

Limited information now available to my Office from complaint cases and investigations lends support to the Sunday Times allegation. I am particularly concerned that there may be an established market in operation through which confidential personal information can be obtained. However, further wide enquiries would be appropriate before firm conclusions could be reached.

The newspaper reports describe activities which may involve criminal offences under the Data Protection Act. It is an offence under Section 5(2)(d) of the Act knowingly or recklessly to disclose personal data to any person not described in a data user's register entry. Such an offence can be committed by the servant or agent of a data user as well as the data user itself.

Investigations carried out have not, so far, produced evidence which would support a prosecution for such an offence. That is, perhaps, not surprising. There are difficulties in obtaining such evidence. Investigations can reveal how a disclosure occurred, but, particularly where there has been deception by a third party, not reveal to whom the disclosure has been made. The fact that a third party may have breached the security of a data user does not necessarily mean that the data user has been reckless. In any event, if a data user is registered to disclose to the type of organisation concerned, for example enquiry agents, then there can be no offence. Many data users may register such a disclosure category because it is appropriate for their normal business activities.

The problems arising from the presence of a market in personal data might perhaps best be tackled by directing attention to those who operate in this market. The Data Protection Act does not, itself, stop or restrict third parties from obtaining access to personal data without the authority of the data user. Nevertheless, I have sought advice as to whether it is possible to prosecute a third party for an offence linked to, if not under, the Data Protection Act.

What appears to have happened in some of the complaint cases is that third parties have deceived employees of the data user into thinking that they had legitimate

access to the data. I have sought counsel's opinion as to whether it is possible to take action against a third party on the grounds of aiding, abetting, counselling or procuring an offence under the Data Protection Act, even though the person who committed the principal offence had no intention of doing so. Whilst leading counsel has advised that such prosecutions may prove possible in certain circumstances, I cannot regard them as any adequate answer to concern about the activities of third parties.

Besides its offence provisions, the Data Protection Act also requires data users to conform to the Data Protection Principles. The Eighth Principle requires data users to have appropriate security measures to protect the personal data they hold. Where complaint cases raise questions about the security surrounding personal data, these are taken up with the data users concerned. Recent investigations, for example, have led to one major data user making improvements in its security procedures to protect against unauthorised access to personal financial information. My policy is to obtain compliance with the Data Protection Principles without embarking on enforcement actions where this is possible. However, I use the enforcement powers of the Act to bring about required changes where this is necessary.

I have no power to inspect or audit computer systems, but do seek to assist and encourage data users to adopt good practices. To this end I have written to the Chief Executive Officers of the major banks asking for their co-operation, firstly in reviewing their own security measures and secondly in making arrangements for my staff to discuss the matter with appropriate senior personnel. I have been pleased at the positive responses I have received. In taking this step I make no implication that there are problems within any of these banks or that the banking industry is the only sector I may ultimately approach in this way. I have also met the Director General of the British Bankers Association (BBA) and have been interested to learn that the BBA has already formed its own group to review and advise on appropriate security methods.

Another factor to consider is the growing trend towards the widespread dissemination of personal data. This may entail the disclosure of potentially sensitive information – for example the disclosure of financial information to and by credit reference agencies. Some of the personal data which are the subject of complaints may have been disclosed from information services of this nature.

The Data Protection Act does not limit disclosures of data, provided such disclosures are in accordance with the data user's register entry. The Third Data Protection Principle which, on the face of it, limits disclosures to those compatible with the purposes for which personal data are held, is effectively negated by its interpretation. I have identified this point already in an earlier report to Parliament and have urged the tightening of the law in this respect. I understand that this has been accepted in principle by the Government, although publication of the draft European Community Directive on Data Protection has put a moratorium on any amendments to domestic law until the final form of the directive is known.

In conclusion, the Data Protection Act can go some way to alleviate the concerns which have been raised, particularly by helping to establish appropriate levels of computer security. But, however good it may be, no security is perfect and it may be that sanctions are also appropriate to deter unauthorised access to personal data by third parties. The Act may also have a role in this respect, but only via a "related" offence which is untested and proving which would give rise to considerable evidential difficulties.

The Computer Misuse Act 1990 may be of some relevance in this context, but my provisional view is that there may well be a potential loophole in the law in respect of the regulation of unauthorised access to personal data by third parties, for example, enquiry agents.

Ministers and Parliament may wish to consider whether there is a need for such regulation and whether current law is sufficient. Such a consideration might be founded on an enquiry into the nature and extent of the trade in personal data apparently revealed by the Sunday Times articles. This matter raises issues of public policy and law which lie outside the statutory cover of the Act and beyond the powers and resources of my Office.

(b) The Police and Criminal Justice System

(i) *The Content and Lifespan of Criminal Records*

The report of a Home Office Efficiency Scrutiny of the National Collection of Criminal Records was published in October 1991. One of the recommendations of this report was for the establishment of a single National Criminal Records System (NCRS) under the supervision of an agency independent of the police. At present, criminal records are held on local police force computers as well as, or in addition to, the national system maintained by the National Identification Bureau. Although no decision has yet been taken in regard to the independent agency, moves have begun to establish a single National Criminal Records System on the Police National Computer (PNC2).

This has re-opened the issue of the length of time for which criminal records should be retained and the attendant criteria under which records should be deleted (or "weeded"). At present I have an agreement which the Association of Chief Police Officers (ACPO) which, in essence, provides for the deletion of records after fixed periods of time. Certain "triggers", for example re-offending, cause the retention of records beyond those periods. The details are set out in the ACPO Code of Practice for Police Computer Systems (the Code) which was published in 1987. Broadly speaking the periods relate to different categories of crime, the sentence imposed and the conviction record of an individual. These periods, which had previously been agreed by the police and the Home Office, do not seem to have been based on any specific analysis of conviction and re-offending experience.

The Home Office Scrutiny accepted my argument that a computer-based NCRS should be used to develop a more sophisticated assessment of appropriate weeding criteria and periods for the retention of records. However, such an assessment will clearly take some time. In the meantime I have been approached by ACPO with proposals to revise the currently agreed criteria. A number of reasons have been advanced for wishing to do this including the prevalence of certain types of serious offence, changes in sentencing policy and practice by the courts and the greater use of cautions by the police.

The ACPO proposals would have extended the time for which criminal records could be kept for many types of offence. A retention period of 20 years since the last conviction would have become the norm for all types of offence committed by adults. There would also have been more categories of offence which would cause this period to be extended up to the age of 70, when it would be reviewed. The time for which a record of cautions would be kept would be extended from 3 years to 20 years. Finally, it was proposed to keep information on acquittals.

The arguments made for these changes were not based on any statistical assessment as, to my knowledge, no relevant statistical information was available. Rather, they were based on the "feel" of serving police officers. Nevertheless, even in the absence of other supporting argument, the views of those undertaking policing work demand serious consideration.

The proposal for the retention of details on cautions caused me concern. Cautions are used much more than was the case a few years ago and for more serious offences. However, I felt that the lack of information on the rates of recidivism seriously questioned the proposal that caution details should be retained on the same basis as convictions. On the other hand I did feel that the move towards the increased use of cautioning did raise legitimate questions as to whether the current 3 year retention period was appropriate.

I and my staff have had several helpful discussions with ACPO representatives. The proposals have been modified and the following are the changes to the current Code on which I hope to reach agreement:

— convictions involving circumstances of indecency or violence, trafficking in drugs and possession of class A drugs would be added to the list of those triggering retention beyond 20 years after the last conviction. This recognises the increasing concern in society about these types of offence.

— cautions would be retained initially for 5 years, with a commitment to analyse recidivism rates before the end of the 5 year period. This would enable the 5 year period to be reviewed on a proper basis and be retained, reduced or extended as appropriate.

The discussions also ranged over the retention of data on acquittals. It does not seem appropriate to retain this kind of information in a system which purports to contain a record of criminal convictions. Both ACPO and I agree that there is no general case for such a retention. However, there may be some exceptional circumstances which will need further consideration.

For example, section 6(3) of the Sexual Offences Act 1956 points to the need to retain certain information. This relates to circumstances where a man under the age of 24 has been acquitted of having unlawful sexual intercourse with a girl under 16 on the grounds that he believes her to be over that age and has reasonable cause for that belief. The need to retain information arises because this defence can be used only once.

A similar need to retain information may arise under section 27(3) of the Theft Act 1968 in respect of evidence of the possession of stolen property in a case where the accused person was acquitted of a charge of handling stolen goods.

The new criteria for criminal record retention and weeding may be published in the revised Code (see below). However, I note that there was Parliamentary debate on these matters when the original criteria were established and both ACPO and I feel it appropriate first to bring any agreement reached to the attention of the Home Office.

(ii) *Putting Old Criminal Records on Computer*

A further element of the National Criminal Records System posing a potential data protection concern relates to the back record conversion of the National Identification Bureau's existing manual records. Due to the numbers and the costs involved it is possible that these records will be converted into computerised form overseas before entry on NCRS. In these circumstances the data would be controlled from the United Kingdom and be intended to be used in the United Kingdom. They would, therefore, be subject to the requirements of the Data Protection Act. I have drawn the Home Office Police Department's attention to the Eighth Data Protection Principle which requires appropriate security for personal data. The department has indicated that, whilst as yet no decision on back record conversion has been taken by Ministers, my advice will be sought if conversion is to take place overseas.

(iii) *Automatic Fingerprint Recognition*

A further element of a criminal record system is the taking and retention of fingerprints. Recently technology has been developed to allow for the automatic comparison of fingerprint records and those taken from the scene of a crime. The National Collection of Criminal Records does not currently include such a facility although the Scottish Criminal Records Office has introduced one in relation to records in Scotland.

A Consortium of some 39 police forces in England and Wales has been established to provide automatic fingerprint recognition (AFR) facilities. This has involved the inclusion in a central collection of each force's set of fingerprints and unidentified scene of crime marks. Whilst the introduction of AFR technology does not of itself pose any intrinsic data protection problems, issues relating to wider compliance with the Act are still relevant.

One area of particular concern centres on the period of time for which fingerprint details would be retained and whether this accords with the requirements of the Sixth Data Protection Principle. This principle requires that information should not be kept for longer than necessary. The periods currently proposed by the Consortium differ from those for conviction records set out in the ACPO Code of Practice for Police Computer Systems. Discussions are underway to resolve the situation. I hope that a satisfactory conclusion will be reached, but until this time I am holding back the acceptance of registration applications from a number of Consortium members.

(iv) *Code of Practice for Police Computer Systems*

In 1987, a Code of Practice for Police Computer Systems was produced by the Data Protection Working Group of ACPO. I was pleased to welcome this valuable initiative in a foreword to the code. As can be seen from my comments on criminal record and fingerprint developments, a code of practice does need to be kept under periodic review to ensure that it continues to remain relevant. Discussions on this have begun with ACPO and I hope that the revision will be published before the next Annual Report.

(v) *Prosecution of Police Officers*

Complaints about police officers are reported by police forces to the Director of Public Prosecutions (DPP). Where the complaints are relevant to the Data Protection Act, it is then for the DPP to decide if a case exists for prosecution of the officer concerned. The prosecution is then taken by the Crown Prosecution Service rather than my Office.

It is an offence under the Data Protection Act for servants or agents of a data user knowingly or recklessly to use or disclose personal data in a manner inconsistent with that data user's entry in the Data Protection Register. Police officers who, for example, used police data for their own personal purposes might face prosecution for an offence. The decision in a recent Court of Appeal Case, referred to in Section 4, may affect future prosecutions for such offences.

There have been a number of successful prosecutions of police officers. However, the DPP has expressed a particular concern about the difficulties in achieving such successes. This stems from the wording of the standard registered purpose for policing. The wording, which governs the uses the police may make of personal data, has proved to be too broadly framed. Consultations with ACPO have resulted in agreement on amendments which tighten the standard purpose description. The amendments will be implemented shortly and I hope that this will overcome some of the current difficulties in taking prosecutions under the Data Protection Act against those who misuse police data.

(vi) *HIV/AIDS Markers on the Police National Computer (PNC)*

Conviction records held on the PNC allow for the inclusion of a warning signal to alert police officers to potential risks to themselves or others. One of the standard warning signals available indicates "may be a hazard to others as a carrier of a contagious disease" and this can be supplemented by an indication of HIV/AIDS status.

I drew attention to this matter in my last Annual Report. As a result of a complaint, I considered whether such an indication of an individual's possible HIV status was excessive or irrelevant for policing purposes and therefore a breach of the Fourth Data Protection Principle. Having taken into account information from a variety of sources including, in particular, that from the Government's Advisory Committee on Dangerous Pathogens, I concluded it was not. However, I recognised that this was a rapidly developing subject and undertook to continue to keep it under consideration.

Since then my staff have participated in a Home Office working group, comprising a variety of participants including representatives of the police service. This working group has drawn up guidance for the police service on HIV/AIDS which has now been issued as a Home Office Circular (113/92).

The circular reflects recent advice from the Government's Chief Medical Officer. The conclusion is that the best protection for police officers lies in their adoption of standard hygiene procedures whenever circumstances arise which may bring them into contact with blood and body fluids. The practice of relying on identification of those with HIV is an inadequate method of protection against infection and may tend to undermine the adoption of standard procedures.

The circular therefore recommends that police forces should set up the necessary training and education to establish standard hygiene procedures and should cease the practice of recording an individual's HIV status on police records. Police forces should aim, where possible, to achieve deletion of HIV/AIDS warning signals by the end of 1993.

In the light of these recommendations I have reviewed the position I took last year. The new factor is that there is now a firm policy on procedures, which should be adopted by police forces, to avoid the risk of HIV infection. Once those procedures are in place, whilst I would look at the facts of each particular case, the holding of HIV markers would seem to be irrelevant. Such markers would also possibly be excessive in view of the danger that they may encourage a false sense of security. This might undermine the hygiene procedures and put police officers at risk.

I have concluded that I should hold to my original view until there has been sufficient time for the necessary training and education activities for police officers to be put in place. I will discuss relevant dates with ACPO, but would expect an early development of the required courses and materials.

(vii) *Enforced Access to Criminal Records*

I have commented before about the practice of requiring individuals to exercise their rights of subject access in order to reveal their criminal records to potential employers or licensing authorities ("enforced subject access"). It may well be proper to examine the criminal convictions of those applying for certain types of employment or particular licenses and, indeed, the Road Traffic Act 1991 allows this for taxi drivers. However, access to criminal records should not be achieved by a misuse of the rights given to individuals under the Data Protection Act.

I have previously recommended that the practice of enforced subject access be made a criminal offence. I recognise that the Act is unlikely to be amended until the European Community's proposed Data Protection Directive has been finalised, but I have again approached the Minister of State at the Home Office to see if earlier action could be taken to end this abuse.

The Minister has informed me that he does not feel the time is yet right to introduce the necessary legislative steps, particularly as the Government is reviewing the general question of access to criminal records. There is also the possibility that the European Community Directive may require member states to place a prohibition on enforced subject access. The latest draft of the proposed directive, published subsequent to the Minister's response, does give individuals a right to resist enforced subject access.

I await the Government's review of access to criminal records with interest. In the meantime I will seek to monitor whether this misuse of the Act continues to grow. There is already evidence of greater numbers of enforced subject access requests to both police and national insurance records.

(viii) *Computer Developments for the Criminal Justice System*

The Committee for the Co-ordination of Computerisation in the Criminal Justice System (CCCJS) continues to press forward with work to rationalise the development and use of computer systems. Views have been given for a consultancy report on data protection and security commissioned by the Committee. I have been encouraged that my Office has now been invited to participate in the CCCJS User Panel. This panel is addressing the appropriate level of data protection safeguards that data users will need to adopt to permit their connection to the system.

(c) The Health Service

The Management Executive of the National Health Service (NHS) has recently launched an information management and technology strategy for the NHS in England. The aim of the strategy is to ensure that information and information technology are managed as significant resources for the benefit of individual patient care as well as for the population as a whole. Key principles behind the strategy include the development of "person-based" systems which hold individual healthcare records; greater integration between different NHS computer systems; and an extension of information sharing. Amongst the components to be developed are a new format NHS number, shared NHS Administrative Registers and a system of NHS-wide networking.

I welcome the assurance by Sir Duncan Nichol, the Chief Executive of the NHS Management Executive that there will be discussions with representatives of the healthcare professions and other interested parties about the implementation of the strategy. Discussions will include the safeguards required to maintain the confidentiality of personal health information to ensure that it will be available only to those who need to know it and who are authorised to know it. I am also encouraged by the general level of interest in data protection and confidentiality within the NHS, evidenced in part by the extent to which my staff are called on to contribute to a wide range of seminars on this topic. It is very important that this level of support and interest translates into adequate safeguards as the new NHS systems develop. The sensitivity of personal health data demands no less.

(i) *The Internal Market*

In my last Report I referred to the development of the internal market in the NHS. This has led to contracts for the provision of health care between

purchasers and providers and an associated flow of patient information in what are termed "contract minimum data sets". This information is used both to support the purchaser's role in the internal market and for planning and management purposes. During the year my staff completed an investigation to consider whether the collection, content and use of these data sets could lead to contraventions of the requirements of the Data Protection Act.

The investigation has revealed the need for providers and more particularly purchasers to review their practices to ensure compliance with the First, Fourth and Eighth Data Protection Principles. These Principles require that personal data be "fairly obtained", "adequate, relevant and not excessive" and kept securely. Particular attention needs to be given to the way in which patient information is obtained, the requirement for purchasers to hold patients' names and addresses and the holding of data on marital status and ethnic origin. A detailed report of the investigation has been published and over 900 copies of this have been distributed. The findings are summarised in Appendix 3.

I am now taking forward the conclusions of the investigation. Discussions have started with the NHS Management Executive on the implications of the report and the role the Management Executive can play in encouraging sound data protection practices at purchaser and provider levels. The removal of "marital status" is under consideration and I have been assured that I will be consulted before "ethnic origin" is introduced as a data item. Arrangements will be made to provide detailed guidance on the application of the "fair obtaining" requirements of the First Data Protection Principle in the NHS.

(ii) *The NHS Number*

A decision has now been taken to re-issue National Health Service Numbers. These will become the primary reference for health records in England and Wales. During the consultation leading up to this decision I expressed concern that the format of the new number might compromise patients' confidentiality by incorporating recognisable personal information such as date of birth. I am pleased that my concerns were recognised in that the format will now be purely numeric, unstructured and include a check digit.

The Community Health Index (CHI) numbers used in Scotland and Northern Ireland already have a format that includes an individual's date of birth. These numbers will be interchangeable with the new NHS Number for England and Wales. The cost and administrative burden of reissuing existing CHI numbers in a format that does not reveal personal information may not be outweighed by the gains for individual privacy. However, consideration should be given to issuing future CHI numbers in the same format as the new NHS number. This would gradually bring all numbers to the same standard. My staff will be discussing this possibility with the Scottish and Northern Ireland Offices.

In my Sixth Report I raised concerns about the possibility of the National Insurance Number becoming a de facto common identifier without Ministers and Parliament having the opportunity to consider whether a national identification system should be established. The same concerns now arise with the new NHS number. It will be issued at birth, will be well maintained, actively used and provide a unique identification number. Pressures are likely to arise for its use for non-NHS purposes. In effect it could become a de facto national identity number.

The Department of Health and the NHS Management Executive have made it clear that they share a wish to ensure that the new number is securely held and used only for NHS purposes. They have stated that, in the unlikely event that it proves necessary to pursue unauthorised use of the new NHS number, it will be possible to do so on the grounds that the NHS numbering system will be Crown Copyright.

Experience with the National Insurance Number leads me to question whether it is unlikely that others will wish to use the new NHS number for their own purposes. Crown Copyright may prove an expensive and cumbersome remedy to counter possible uses of the number. Also, Crown Copyright does not prevent the use of the NHS number by other Crown Agencies.

I am disappointed that the Secretary of State has not felt able to respond more positively to my view that statutory control of access to and use of the new NHS Number is appropriate.

(iii) *NHS Administrative Registers*

Work has started on the development of a set of nationally linked NHS Administrative Registers. These will be shared population registers containing basic details about individuals such as name, address, sex, date of birth, NHS number and NHS organisations the individual is registered with. Although the data will be primarily administrative rather than clinical it might nevertheless be sensitive, for example revealing details of NHS organisations a patient is in contact with. It is intended that information from the registers will be available throughout the NHS on a "need to know" basis.

There have been discussions on the data protection implications of these registers with the NHS Management Executive. I anticipate there being further consultation with my Office as the main areas of concern are clarified. Issues to which particular attention is being given include the extent to which information on an individual's former names and previous addresses will be held; the methods through which access to the registers by NHS staff will be controlled; and arrangements to ensure the accuracy of the information recorded. I am anxious that the information that will form the registers should be obtained fairly as required by the First Data Protection Principle and that any rights patients may have over their information are not compromised. Decisions will be needed on the circumstances, if any, in which non-NHS organisations such as local authorities, the police and researchers are able to gain access to the registers.

(iv) *The Confidentiality of Health Information*

In my Fifth Annual Report (1989) I referred to work which the Interprofessional Working Group in the medical sector had carried out to produce a draft Code of Confidentiality of Personal Health Information. A debate was continuing as to whether the Code should have statutory force or not. In my Seventh Report (1991) I reaffirmed my support for adoption of the Code which would set strong constraints on the use and disclosure of personal health information.

At the same time I expressed some disappointment that the Department of Health had not supported the introduction of statutory provisions. The Department was working on its own draft non-statutory guidance and I had been assured I would be consulted as to the data protection implications. Unfortunately, the Department has not yet been able to publish this guidance.

In the context of the internal market, I have welcomed a Code of Practice for the Handling of Confidential Patient Information in the Contracting Environment issued by the NHS Management Executive. However, I remain concerned that the Department of Health's much wider guidance on the confidentiality, use and disclosure of personal health information is still not available. The sharing of information between the NHS, local authority social services departments and other agencies as required from April 1993 by the community care reforms, makes the need for clear, comprehensive guidance even more pressing.

One recent reason for the continuing delay might be the Department of Health's approach, late in 1992, to discuss with me the inclusion of guidance on the fair obtaining of information from patients. I notice that the Government recently announced, in a House of Lords debate, that draft guidance on the confidentiality of health data and the press would be issued in advance of finalisation of guidance as a whole. The Government has now followed up by issuing a draft circular for comment. I would not wish to hold matters up on the single point of fair obtaining. If it proves not to be capable of resolution within a reasonable period I will ask the Department of Health if it could consider releasing the other parts of the draft guidance.

(v) *The Case for Statutory Protection*

I have referred to the increasing need for safeguards to ensure that developments in the NHS do not compromise the confidentiality of sensitive health information. I have doubts whether the common law, non-statutory guidance or professional codes alone will be sufficient. The common law duty of confidence is complex and does not appear to have been tested in circumstances such as the wide use of health information in the NHS. In any case, it is a cumbersome and expensive remedy for an individual. As I understand it the Department of Health's proposed guidance will only be applicable in the NHS and will rely for enforcement on the contractual duties staff owe to a multiplicity of employers. Professional codes may well vary in content and enforceability and they will not cover all those dealing with health information.

It seems appropriate for there to be clear, enforceable, and generally applicable controls on the collection, use and disclosure of personal health information. It may be that only statute law can provide these.

The Data Protection Act enabled the United Kingdom to ratify the Council of Europe Convention for the Protection of Individuals With Regard to Automatic Processing of Personal Data. Article 6 of the Convention provides that sensitive personal data, which includes that concerning health, may not be processed unless domestic law provides appropriate safeguards.

The Consultative Committee established under the Convention has recently given a formal opinion on Article 6. It concludes that "appropriate safeguards" should be understood as any measure protecting sensitive data which goes further than the minimum protection which, under the Convention, must be given to non-sensitive data. Whether the Data Protection Act does, in any case, go further than this minimum level is a matter for careful consideration. If further protection is required, then Section 2(3) of the Act allows an order to be made to strengthen the Data Protection Principles in their application to personal health data.

(d) Local Government

(i) *The Council Tax*

The council tax came into being on 1 April 1993. In the course of preparing for the new tax my staff worked closely with officials from the Department of the Environment, the Department of Social Security, the Welsh Office and the Local Authority Associations to develop data protection guidance for local authorities. A council tax practice note on information and data protection has been circulated. This is one of a series of nine such notes published by the Department of Environment.

The practice note gives general guidance on the requirements of the Data

Protection Act and the specific registration requirements arising from the council tax. It also relates the 'fair obtaining' requirements of the First Data Protection Principle to the information gathering powers of local authorities. The Fourth Data Protection Principle requires that personal data be "adequate, relevant and not excessive". The practice note suggests those types of information which are likely to meet this requirement and those which are not. Model inquiry forms are provided for use by local authorities seeking to identify those who are liable to pay the tax and those who qualify for the award of a discount.

My staff have given both written and telephone advice to numerous local authorities and others. They have addressed more than twenty seminars of council tax practitioners around the country. I welcome the extent to which early and detailed attention has been given to the data protection issues involved. Whilst I have investigated some complaints from the public about the council tax, these complaints are neither as numerous nor raise matters of the same substance as those I received about the community charge. Indeed, some community charge problems are only just being cleared up.

In my last Report I indicated that the Government had taken the view that, as a matter of policy, copies of council tax valuation lists would not be available for sale commercially. I am aware that the Department of the Environment has received a number of enquiries asking whether the lists can be sold. I welcome the Department's clear advice that, beyond individual rights of inspection, a local authority cannot sell either these lists or information from them.

(ii) *Housing and Council Tax Benefits*

In August 1991 I issued a consultation paper outlining my initial concerns about the way in which computerised records are used by local authorities to administer government benefits. Many detailed responses were received. My staff subsequently took part in a series of meetings with the Department of Social Security (DSS) and the Local Authority Associations.

Whilst I have not been in a position to make progress as quickly as I originally hoped, I have recently been able to forward draft data protection guidance to the DSS. This draft guidance highlights the requirements of the First Data Protection Principle that personal data be "obtained fairly" and "processed lawfully" and the requirement of the Fourth Data Protection Principle that personal data should be "adequate, relevant and not excessive". It addresses the extent to which individuals supplying information on claim forms should be made aware that, in some instances, the information collected from them may be used for purposes unconnected with their claim or may be disclosed outside the local authority. The draft guidance also questions the holding of certain information about claimants including National Insurance Numbers of those not receiving income support, employment details, financial details of non-dependents, marital history and treatment in hospital.

Further discussions are underway with the DSS and the Local Authority Associations which I hope will lead to the issue of clear, practical advice for the benefit of practitioners. These discussions cover not only the implications of the draft guidance for the administration of benefits but also the way in which the guidance will be disseminated.

(iii) *Social Policy Research*

Local authorities and housing associations are from time to time asked to provide samples of housing tenants or prospective tenants in connection with social policy research. A sample might be drawn from a particular sub group such as tenants with significant rent arrears. Names and addresses of individuals in the sample are passed to independent research organisations who

interview the individuals or send them questionnaires. The research organisations then pass aggregated information to government departments, most usually the Department of the Environment (DoE).

I have received enquiries from local authorities concerned as to the data protection implications of this practice. As a result I made an approach to the DoE. I have subsequently been involved in detailed discussions with representatives of relevant government departments and research organisations about the application of the "fair obtaining" provisions of the First Data Protection Principle in these circumstances.

It has been accepted that there is a need for local authorities to inform tenants or prospective tenants that information they provide in connection with their housing needs might be passed on to research organisations. In addition there will be some cases where a local authority, seeking to ensure that housing information is fairly obtained, will have to give a tenant or prospective tenant the opportunity to "opt out" of the disclosure of his or her information for research. This will occur with those clients of a local authority housing department who do not, in practice, have other sources of housing available to them such that they could decline to provide information.

Whilst a local authority will – solely on account of the Data Protection Act – only be required to offer an "opt out" to those clients who have no real choice over where they seek housing, it is clear that there might be practical difficulties in an authority's identifying and applying different standards to different groups of clients. A prudent local authority might therefore conclude that the only way it can ensure that an opt out is provided in those cases where it is required is to offer the facility to all tenants or prospective tenants.

I am taking steps to ensure that local authorities and housing associations are made aware of the fair obtaining requirements appropriate to this activity.

(iv) *Community Care Reforms*

In referring to issues in the Health Service I mentioned the impact of the community care reforms. From April this year local authorities have taken on responsibilities for assessing individuals' needs for care in the community and for arranging appropriate care, including residential and nursing home provision. These developments are inevitably giving rise to a greater sharing of information on patients and clients between the NHS and local authority social services departments.

In some cases personal data on individual patients will be under the control of both a social services department and an NHS Authority or Trust. It is essential that both organisations are clear as to who has the responsibilities of a data user under the Data Protection Act. In situations where there is any doubt I recommend that the parties enter into a contract or other formal agreement which clarifies matters.

Any arrangements for the sharing of personal data should take full account of the requirements of the Data Protection Principles. In particular individuals should be made aware of who will share this data and for what purpose. The information held should be no more than either the relevant NHS organisation or the social services department needs to fulfil its functions. Security measures are required that are appropriate to the sensitivity of the personal information that is involved. I look to the authorities concerned to develop the necessary standards and practices.

(v) *Computing in Schools*

In my last Report I outlined the reasons why many governing bodies and

headteachers of local education authority (LEA) maintained schools have to register under the Data Protection Act as data users in their own right. My staff assisted officials of the Department for Education (DFE) and the Welsh Office in drafting guidance for issue to LEAs and LEA maintained schools. Similar guidance is issued to new grant maintained schools in England.

There have been over 20,000 applications for registration from governing bodies and headteachers. There has been a wide range of enquiries from schools and detailed advice and assistance is provided wherever possible. I am encouraged that most governing bodies and headteachers are clearly aware of the requirements of the Data Protection Act and have recognised their responsibilities for registration.

However, I am concerned that some 18 months after the DFE's guidance was issued there appear to be a significant number of governing bodies and headteachers who, whilst qualifying as data users, have not yet registered under the Act. To be a data user without being registered is a criminal offence, now attracting a fine of up to £5,000 in a magistrates court. I will be taking steps to identify where these failures to register at school level exist and to rectify any omissions. I note that the number of registrations varies substantially across different education authorities.

So far as Scotland and Northern Ireland are concerned I have been examining the relevant legislation. It appears to me that, in Scotland, control of personal data held in maintained schools generally rests with the Regional and Islands' Councils, as education authorities, rather than with individual school boards or headteachers. However, in Northern Ireland there is a substantial element of control that rests with boards of governors and school principals. I have been concerned about delay in issuing guidance from the Department of Education for Northern Ireland. However, I am pleased to have recently received assurances that formal guidance should be issued to boards of governors and principals around the time this Report is published.

Parliament has recently been considering a new Education Bill. Amongst other provisions the Bill provides for the governing bodies of LEA maintained schools in England and Wales to become corporate rather than unincorporated bodies. A corporate governing body will be a different legal "person" from its unincorporated predecessor. If it holds personal data it will have to take out a new registration on the date of incorporation and pay an additional registration fee. This will place a considerable financial and administrative burden on governing bodies without any counterbalancing benefits for the accuracy and completeness of the Register. I have therefore proposed to the DFE that an additional clause should be incorporated into the Bill transferring the data protection registration from the existing to the new governing body.

(e) Data Protection and the Media

When considering the position of data protection and the media, privacy and freedom of expression – two important human rights – bump up against each other. There has, of course, been much wider debate about privacy and the press outside the context of data protection. Data protection was mentioned in the Calcutt Review*. It was suggested that there should be a further examination of the role which the Data Protection Act 1984 might play. I believe this arose from evidence put in by my Office.

Broadly, my view is that modern highly automated newspaper production systems are within my jurisdiction. In that case, a newspaper publisher, as any data user, must

* Department of National Heritage Review of Press Self-Regulation by Sir David Calcutt QC, published by HMSO, January 1993.

register and comply with the eight Data Protection Principles. In particular, he must hold accurate data and obtain information fairly and lawfully. I might, for example, take the view that telephone interception was an unfair means of obtaining information; in which case I could serve an Enforcement Notice to secure a remedy for this breach of principle. Although this may not be the most straightforward way of regulating these issues, I do believe that the Data Protection Act would have a role to play if complaints were made to me in appropriate cases.

As can be seen from Section 2, the use of personal data by the media is also a matter of consideration in the proposed European Community (EC) Directive on Data Protection. I am concerned that any exemptions given to the media as a result of an EC directive should only be such as are strictly necessary to reconcile privacy rights with freedom of expression. If subject access exemptions were specifically granted to investigative journalists, for example, it would be difficult to understand why these should be wider than those available to the police. The media should not simply be granted sweeping exemptions from legislation which protects individuals.

There are no special exemptions for the media in the Data Protection Act 1984. To the best of my knowledge this has not caused any problems. This seemed to be confirmed at a meeting during the year with representatives of the Independent Television Association, ITN, Channel 4 and the BBC. The Deputy Registrar has subsequently met with representatives of the Newspaper Society and the Newspaper Publishers Association.

I hope to continue discussions with the media towards the end of the year when I expect the provisions of the proposed EC directive will have become clearer.

(f) The Code of Banking Practice

The Code of Banking Practice was published in December 1991 and came into force on 16 March 1992. It followed the Banking Services Review Committee report on banking confidentiality and provided a self-regulatory, rather than statutory response to the conclusions of that report. It relates to banks, building societies and card issuers.

From the data protection viewpoint the two relevant parts of the code relate to customer confidentiality and the marketing of services. These are covered in Sections 6 and 8 respectively of the code.

Paragraph 6.1 of the code states that:

> "Banks and building societies will observe a strict duty of confidentiality about their customers' (and former customers') personal financial affairs and will not disclose details of customers' accounts or their names and addresses to any third party, including other companies in the same group, other than in the four exceptional cases permitted by the law."

The four exceptions are known as the Tournier rules. Disclosure of such information is permitted where:

— a bank or building society is legally compelled to do so;

— there is a public duty to disclose;

— the interests of the bank or building society require disclosure;

— disclosure is made at the request, or with the consent of the customer.

Paragraph 8.1 of the code states that:

> "Banks and building societies will not pass customers' names and

addresses to other companies in the same group, in the absence of express consent."

A Review Committee, chaired by Sir George Blunden, has been set up to monitor the operation of the code of practice. In February 1993 the Committee started its first review of the code. I am pleased to have been asked to comment and I have passed the following views to the Committee.

The first concern is that some banks have made it a condition of trade that individuals give their express consent for information about them and their accounts to be passed to other organisations. These organisations may primarily be other companies in the same group. That does not necessarily mean that these other companies are involved in banking activities. The benefit to individuals under section 8.1 of the code is clearly negated, as far as these banks are concerned, if a customer cannot have an account unless he or she gives consent to the very disclosures the code is supposed to govern.

Secondly, the protection given by paragraphs 6.1 and 8.1 has been undermined by the fact that many banks employ "host mailing". By this technique, they mail selections of individuals on their own databases with offers of goods and services from other companies in their groups. The banks' customer information is not disclosed to the other companies, although they may ultimately come into possession of it. A simplistic example of this might be where a bank mails a financial service offer on behalf of another company in the group. It does so only to those customers with a deposit account balance of at least £5,000. The other company will know that any bank customer responding to it has such a balance. This information will effectively have been passed from the bank to the other company without its customers' knowledge, let alone consent. In the current code, emphasis has been placed on the disclosure of information. However, it can be argued that a bank's duty of confidentiality can be breached not only by disclosure of customer information, but by the use of such information. This second concern might be met if the requirement for customer consent in the code constrained not only disclosures, but uses of a customer's information.

Thirdly, some banks, building societies and card issuers disclose both "black" (where an account is in default) and "white" (a normal account) information to credit reference agencies. There must be a question mark as to how these disclosures of information by banks to credit reference agencies are permitted by the code or under the Tournier rules. It may possibly be argued that disclosing information to credit reference agencies in the interests of other banks can be said to be properly required in the interests of the disclosing bank because of a "quid pro quo" arrangement. I feel that this argument may be difficult to sustain.

(g) Free Insurance Offers by Banks and Building Societies

My attention was drawn recently to promotions being undertaken by a number of banks and building societies in conjunction with an insurance company. The promotion offered customers a period of free accidental death insurance. I had information in relation to one particular bank which led me to believe that the main objective of the promotion was to improve the quality of information held on customers. In particular, it was intended to obtain customers' dates of birth where these were not already held. In view of this I questioned whether the information was being obtained fairly.

Customers taking advantage of the offer were to be asked to complete an application form giving brief personal details including their date of birth. The application form contained a notification that information provided might also be used to advise the customer of other services provided by the bank and its related companies. It seemed to me that this notification did not reveal the full purpose for which information was being obtained.

I am pleased to say that the bank concerned offered to include with the proposed mailshot a separate insert with a notification which clearly explained its information gathering purpose. The wording agreed was as follows:

> **"Data Protection Act 1984**
> The enclosed application form requests you to provide certain information. As well as assisting us in providing a service which you might apply for in the application form, the information obtained from you may be used to update and enhance our records. An important purpose of this exercise is to obtain improved date of birth data for our customers which is obtained as part of the response information requested. This exercise should enable us more efficiently to advise you of other services provided by [name of bank] companies in which you might be interested."

(h) The Credit Sector

The amount of work involved in the enforcement actions on the use of third party information has now lessened and attention is being directed to other credit issues.

It is hoped to take part in more regular meetings with the Credit Industry Forum on Data Protection. A recent meeting discussed matters such as:

— the fact that credit reference agencies show an outstanding account as having been written off when the individual has paid the amount due to a debt factoring company;

— the transfer of data between credit reference agencies and the banks. It appears that, in certain circumstances, out of date information is supplied to banks. For example, an account that used to be in arrears but is now paid up will sometimes be reported to the bank as a currently delinquent account;

— credit checks with credit reference agencies which appear to be being undertaken by financial institutions offering accounts that do not give credit;

— the retention of credit card numbers and account numbers by credit reference agencies, particularly when these are disclosed to their clients or as third party information on credit reference files obtained by individuals;

— the use of credit reference information by debt tracing agents;

— the length of time that bankruptcy data are held by credit reference agencies.

(i) Mortgage Information

Regular meetings have been established with the Council of Mortgage Lenders. The Council wishes to extend its Possessions Register, which contains details of houses that have been repossessed by building societies, to include mortgage arrears information. In addition the Council of Mortgage Lenders wishes to set up a Mortgage Applications Fraud Register. In a further initiative, a joint venture between five or six building societies is directed to setting up a Valuations Register which may itself be expanded into a Mortgage Applications Fraud Register. There is a very co-operative attitude on the part of the building societies and detailed advice is being given at the planning stage for all of these projects.

(j) Fair Obtaining of Information

The First Data Protection Principle requires that information to be contained in

personal data must be obtained fairly. The Data Protection Act has had a significant effect on the standards set here in both the public and private sectors. A comment on information which is obtained under statute is included in Section 4(d).

There may be occasions where an individual should be given an opt-out from extraneous uses of information he or she provides to a data user. I have been pleased to see that the British Code of Advertising Practice administered by the Advertising Standards Authority (ASA) sets this standard for direct marketing activities by third parties. However, in general I have taken the view that the Act simply requires that those providing information should be informed, when they supply it, of any extraneous organisations, uses or disclosures which they could not reasonably be expected to anticipate.

There are many different reactions to the issue of fair obtaining. Plainly, some disagree with my view of the law and that will be tested in the appeals to the Data Protection Tribunal referred to in Section 6. The following examples also illustrate a range of responses:

— the Government notification to individuals of the BT3 share offer makes it clear that, if an individual registers with a share shop, he or she may receive offers of other services from that shop. It can be argued that this might be apparent to most individuals and I am pleased, following consultation with my Office that the position has been made clear for all;

— a wide range of organisations is now informing individuals when they supply information that it may be used for mailing purposes by those organisations and others. Many organisations offer a simple opt out from such mailings via a tick-box. However, some make the opt out less easy to exercise by requiring individuals to write in requesting this;

— discussions throughout 1992 led to the introduction of a code of practice which set standards for the fair obtaining of personal data by agencies which accept bookings for theatre and other events over the telephone. A formula was devised to ensure that information is not used about those who buy tickets over the telephone without their being properly aware of extraneous uses and disclosures and being given an opportunity to opt out of these;

— discussions with the principal mail order traders have ensured that they now obtain information, to be contained in personal data, fairly. For example by including statements to individuals who apply for mail order catalogues that their details will be checked with a credit reference agency and that the credit reference agency will retain details of that check. Interestingly, although it has been possible to conclude matters successfully with the individual mail order traders, it has proved very difficult to obtain the same level of agreement with their representative body, the Mail Order Traders Association (MOTA). It is hoped in the near future to re-establish discussions with MOTA to try to enshrine the agreements reached with the individual companies within the industry code of practice;

— individuals completing lifestyle questionnaires may not be aware that the information they provide is going not only to the lifestyle questionnaire company, but also to other companies which have sponsored particular questions. Discussions with one of the largest companies producing lifestyle questionnaires have resulted in enhanced notifications about this point. These advise individuals that information provided in answer to specific questions will be shared with particular organisations.

The proposed European Community Directive on Data Protection referred to in Section 2 may well require that details of uses and disclosures of information be given when it is obtained from individuals. I hope that the progress made over the

last few years can continue, both under the Act and under a directive, with a convergence on high standards of openness, not least those contained in the British Code of Advertising Practice.

(k) Direct Marketing

As indicated in Section 5, there has been a steady decline in the number of complaints received about unsolicited mail. I believe that the Data Protection Act has led to what seems to be a lowering in the irritation caused to many people by what is popularly called "junk mail".

The Act has contributed in two ways. Firstly, through causing greater openness by those who collect and pass on information about individuals for marketing purposes. The discussion of "fair obtaining" above, indicates the sort of progress which has been made. Secondly, by supporting and stimulating the valuable initiative, taken by the direct marketing industry itself, in setting up the Mailing Preference Service (MPS).

The MPS allows people to suppress the use of their names on direct marketing mailing lists. It accords well with my view of the requirement in the First Data Protection Principle that personal data shall be processed fairly. Since the Act came into force, the industry has invested to develop and re-organise the MPS and it now has a "stop list" of over 300,000 households. Those who do not wish to receive unsolicited mail and register with the MPS should find a significant reduction in envelopes dropping through their doors after a period of a few months.

The proposed European Community Directive on Data Protection currently contains a right for individuals to have their details removed from marketing lists. The value of the MPS may well be underlined by this requirement.

(l) Telecommunications

In my last Annual Report I referred to calling line identification (CLI). This is a facility which is becoming possible with the modernisation of telephone networks. It is a technique which, in its simplest form, allows a person receiving a telephone call to read, from a display on the receiving instrument, the telephone number from which the call has been made.

An Appendix to that last report sets out my views on CLI. I pointed to possible advantages and disadvantages of this facility. The advantages fell to the party being called. They were:

— by partially removing anonymity from those making calls, CLI is likely to reduce the number of malicious calls;

— CLI can assist the emergency services in tracing the source of calls, where this is not stated, and could also discourage hoax calls;

— CLI gives the recipient of a call the opportunity to decide, on the basis of the displayed number, whether or not to accept a call;

— transmission of the caller's number creates marketing possibilities for called organisations, through capture of the caller's number and immediate linkage with databases which can provide and capture additional information about the caller.

The disadvantages were for the calling party. They were:

— If the display of numbers were compulsory and universal, the ex-directory system would be prejudiced;

— the threat of malicious calls would be reduced, but the number of unwanted calls (eg. from patients to doctors at home) could increase as the result of the availability of callers' numbers;

— compulsory universal CLI would make the anonymous calling of helplines, or of the police to give information, very much more difficult. It may restrict such calls to those made from public telephone boxes. It could also be a hindrance to organisations such as the police when making calls as part of their duties;

— CLI would be likely to lead to increased numbers of 'junk telephone calls' if the numbers of callers to suppliers of goods and services were 'captured' for later marketing use.

CLI therefore has benefits for the called party, in providing him with extra information about the caller even before the call is accepted. But the question arises as to how best CLI can be implemented without enabling the called party to take unfair advantage of the caller.

I concluded that the introduction of CLI by a United Kingdom telecommunications operator would raise issues within my jurisdiction. These could only be addressed adequately by the introduction of measures to ensure that the use of CLI does not contravene the Data Protection Principles, particularly that requiring the fair processing of personal data. Those measures should include facilities to allow the caller to suppress the display of his number to the called party on a call-by-call basis (per call blocking) or for all calls from his line (per line blocking). Furthermore, those facilities should be simple to use and must not give rise to a direct charge to the subscriber who blocks CLI.

Events have moved on in the last year. Both of the major national network operators, British Telecom (BT) and Mercury, are considering providing CLI on their networks. Both companies have held meetings at which their proposals were explained. I was pleased to be invited to these and to see that the issues which I raised have been recognised. Indeed, there does seem to be a wide consensus across the industry that the legitimate privacy interests of the caller must be taken into account by providing blocking facilities. However, whether the telecommunications companies will wish to provide all the possible blocking facilities remains to be seen.

British Telecom has gone further towards the implementation of CLI by establishing a live trial in Elgin in the North East of Scotland. Selected subscribers on the local exchange taking part in that trial were loaned a call display unit to plug into their telephone line. This provided a CLI display for calls from any other subscriber on the local exchange. All calling subscribers had available a per call blocking facility by which the display of their number could be suppressed by dialling a prefix before dialling the number to be called. A per line blocking facility was also available but was not offered generally to subscribers along with per call blocking.

I was consulted by BT before the trial began and took the opportunity to comment on some of the details. I did not raise any objection to the trial proceeding, though I expressed reservations on some aspects, particularly the approach taken to per line blocking, where I maintain the position I took in my 1992 Report. The trial was concluded at the end of March 1993, and I expect to have the opportunity to discuss the results with BT in the near future.

It seems almost certain that CLI will be introduced nationally in the not too distant future. There does not now seem any likelihood that it could be introduced in an unrestricted form without blocking. However, the debate will continue on what form

the blocking facility should take and how blocking requests will be transmitted across network boundaries. There is also an issue as to how the telephone user population will be informed about the facilities available so that they can make an informed choice as to whether their number is displayed or not. I look forward to taking an active part in that debate and I have already been asked to comment on a proposed code of practice for interconnecting network operators. It is plainly important that privacy protection can be guaranteed across connecting networks before CLI is introduced.

(m) Data Matching

Data matching is the computerised comparison of two or more sets of records. The objective is to seek out any records which relate to the same individual. Where there is such a "match" then the information from one set of records may be transferred to enhance the other set. Alternatively, the information on the matched individual may be extracted for decision and action and may form the basis of a further set of records. This new set may ultimately form a set of "profiles" of individuals drawn from a number of different sources.

There are a number of variations of the technique. For example, records on a single or a selected number of individuals may be sought from a particular file. Alternatively, a set of records may be searched to find all those with a particular set of characteristics. However, there is usually the common point that the sets of records being searched have been assembled for different purposes than that which is the object of the data matching.

Data matching has been commented on by the Home Affairs Committee of the House of Commons and the Government has stated that it will consider proposals I wish to make regarding this technique. I raised this issue in last year's Report and undertook to obtain views from interested parties.

As a first step to obtaining views so that I can respond to Members of Parliament and the Government, I am seeking to gain an understanding of data matching in government departments. To this end I have asked the Permanent Secretaries of the Home Office and the Department of Social Security together with the Chairman of the Board of Inland Revenue if they would be kind enough to provide assistance for a pilot survey of their departments. I welcome the positive responses I am receiving. The objective of the pilot study and subsequent enquiries will be to determine what, if any, data matching takes place in government departments and how this is developed and operated. From this picture, I would look to draft any appropriate data protection guidelines for further discussion.

I have been approached by the Audit Commission which has been engaged in a project to study the potential use of data matching in local authorities. In mind is the objective of establishing the extent of fraudulent claims and the measures that might be taken to reduce these. My staff will be holding further discussions with the Audit Commission as this project progresses.

(n) The Security of Personal Data

The Act requires that appropriate security measures shall be taken to protect personal data. The European Community Draft Directive on Data Protection (see Section 2) reinforces this requirement. As some of the complaints this year illustrate, the use of even simple security methods could help to prevent problems for individuals.

Advice and information on data security will obviously be valuable to computer users. I welcome, therefore, initiatives underway by both the Department of Trade

and Industry (DTI) and the European Commission in this matter.

The DTI points out that, whilst there are a number of guidelines on good information security practice and many company versions of these, there is no consensus document which is generally used to achieve good practice. In the light of this, the DTI is leading a group of major companies in developing a code of practice. The code is planned to have a broad consensus and become a British standard. The first version of the code is likely to be published early in 1994. Subsequently, consideration will be given to an accreditation and certification scheme for data users' information security. The code would be used as the basis for this.

The package of measures proposed by the European Commission in 1990 included a proposal for a Council Decision in the field of information security. The Commission argued that effective information security is an integral part of the protection of the privacy of individuals. For this reason, for the development of the data processing and telecommunications industries and for the completion of the internal market, an active policy for the creation, development and promotion of information security standards was necessary.

The proposed Council Decision was adopted by the Council of Ministers on 31 March 1992. Its principal features are the formulation of an action plan, initially for 2 years, for the development of strategies for the security of information systems and the establishment of a Senior Officials Group on Information Security with a long-term mandate to advise the Commission.

A number of tasks are underway to address specific issues and to do further research. One of the principal objectives is the development of common specifications and standards. On the basis of these, evaluation and certification schemes for information systems security could be developed.

(o) The Population Census

I reported last year that the Census Offices of the United Kingdom were seeking comments on the way the population census should be conducted in future. I expressed concern about a number of the possibilities mooted. They included the establishment of population or housing registers and extracting information from administrative records gathered for other purposes.

Ministers issued a news release in October 1992 saying that the consultation had indicated a general satisfaction with the traditional form of census and that no alternative options would be developed. It was also announced that planning would proceed on the assumption that the next census of population would be held in 2001.

A report on the consultation has been published by the Office of Population Censuses and Surveys (OPCS). The traditional census will remain and the OPCS will continue work on examining how secondary sources of information would be used to supplement the main source. I look forward to continuing consultation with OPCS on the data protection aspects of this work.

4 Determining the Meaning of the Law

The Registrar cannot make a final determination of the meaning of the Data Protection Act; that is the role of the Courts. He does have to make his own decisions as to his views of the meaning of the law in the circumstances before him. In carrying out this function I have tried firstly to arrive at the decision the courts would make, secondly to achieve consistency of view and thirdly to propagate the view arrived at.

During this year, two cases have come before the Higher Courts on points of law arising under the Act. In this section I give information on the Courts' decisions and review a number of my decisions which have wide import. Sometimes these are based on advice from Counsel. The Data Protection Tribunal has not heard any appeals this year and so no new decisions are available from it. Last year I reported the Tribunal's decisions in respect of the enforcement actions appealed by four credit reference agencies. This year I give my detailed view of the effect of those decisions.

(a) Data Protection Registrar v. Francis Joseph Griffin, Queens Bench Division – 22 February 1993

On Monday 22 February 1993, the High Court of Justice, Queens Bench Division heard an appeal by the Registrar against a decision of the Kingston-upon-Thames Magistrates of 1 June 1992. The Magistrates' Court had found the defendant not guilty of holding personal data contrary to Section 5(1) of the Act.

Mr Griffin, the defendant, was a self-employed accountant whose business was the preparation of accounts for clients. He owned his own computer and worked from home. He prepared and dealt with the accounts of clients. His method of working was to receive clients' accounting information in written form through the medium of invoices and other paper records. He would then use this information in a "spreadsheet" computer programme from which he would derive company accounts or private accounts for submission to the Inland Revenue and Customs and Excise for the purpose of VAT, Corporation Tax and Income Tax, by or on behalf of his clients. He had never been registered under the Data Protection Act. When he was interviewed and asked whether he controlled the content and use of the data he said that he did.

The case turned on whether Mr Griffin did actually control the content and use of the data on his computer or whether his clients did so. If Mr Griffin did not control the data he would not be a data user and would not have to register; if he did control them then he was liable to register.

Mr Griffin argued that he could not be said to exercise control as he had no right to use the data in any other way than to produce his clients' accounts. Although he manipulated the data to produce the accounts that did not amount to control.

I contended that, although there were restrictions on the use of the data in terms of contractual and professional limitations, Mr Griffin still controlled the data within

the meaning of the Act. He had a power to manipulate the data and as that manipulation involved the application of his professional skill, judgement and discretion, it went beyond merely acting on instructions given to him and he should be said to control the data.

The Court dealt with the specific question as to whether an accountant who receives "raw" information from his clients, which he puts on computer and processes to produce accounts for other bodies, is a data user. The Court also dealt with the wider question of whether a person can be a data user where there are contractual limitations on his power to use the information he receives.

The Court decided that Mr Griffin was a data user. The Court also agreed that the fact that there are restrictions placed upon the use of information in the hands of a person does not stop that person from being a data user. Therefore, the fact that Mr Griffin was not free to use the data for his own purposes did not stop him from being a data user. I am pleased that the court supported the view I have taken.

The Court gave weight to the fact that Mr Griffin did not act for one client alone; he acted for a number of clients and the relevant collection of data to be considered, therefore, was the collection of the accounts of all the clients. Only Mr Griffin knew of all the data which comprised the collection and had the ability to influence it. The court also attached weight to the fact that Mr Griffin decided what information should be recorded as data and how the data should be manipulated so as to bring the accounts into existence.

On my behalf, Counsel asked the Court not to refer the case back to the Magistrates' Court for sentencing. Without prejudice to the appeal, Mr Griffin had registered under the Act subsequent to the proceedings in the Magistrates' Court.

I have considered the advice currently given in Guideline 2* on this point and feel it has not been materially varied by the case. However, I am planning a revision of the Guideline series in the forthcoming months and I shall be considering whether the current advice should be amplified or extended.

(b) Regina v Brown – Court of Appeal Criminal Division Times Law Report, 4 June 1993

On 28 May 1993 the Court of Appeal Criminal Division heard an appeal by Gregory Michael Brown against his conviction at Maidstone Crown Court. Mr Brown had been convicted on one count of attempting to use, and another count of using personal data for a purpose other than the registered policing purpose. He was a police officer and it was the prosecution's case that he was using or attempting to use data stored in police computers for a private company with which he was associated.

Their Lordships decided that processing the data on the computer did not constitute "use" for the purposes of section 5(2)(b) of the Act. It was necessary for an accused to take some steps beyond merely looking at the data on the computer screen and to make some use of the information within the ordinary meaning of that word to come within the section.

Accordingly their Lordships allowed the appeal. They agreed to certify a question for the House of Lords. The case was brought by the Director of Public Prosecutions (DPP). A full transcript of the case is not yet available to my Office. At the time of preparing this report no decision has been made as to whether the DPP will appeal to the House of Lords.

*There are eight Guidelines on the Data Protection Act 1984 obtainable free of charge from the Registrar's Office.

In considering the appeal, their Lordships stated that the purpose of the statute was to protect the interests of private individuals.

(c) Decisions by the Data Protection Tribunal on Credit Reference Activities

In last year's Report I gave the history of the enforcement actions I had taken against the four main credit reference agencies. These actions related to the provision of information about other individuals (third parties) by the agencies when lenders enquired about the credit record of a loan applicant.

Following the hearing of appeals, the Data Protection Tribunal issued revised enforcement notices to the agencies. These come into effect on 31 July 1993. They broadly prevent the provision of third party information by the agencies to lenders unless there is some relationship of family and residence between the loan applicant and the other individuals. There is the possibility that this provision may be further limited where, for example, there is no financial relationship between the individuals concerned.

The revised notices themselves have to be interpreted against the range of circumstances which may occur. To assist the agencies, I have produced guidance on my own view of the meaning of the notices. This is reproduced in Appendix 4. I shall use this view if I have the occasion to consider whether any of the agencies are in breach of the terms of their notices.

(d) Obtaining Information Under Statute

I have given considerable thought to the meaning and effect of the interpretation provision to the First Data Protection Principle which deals with how information obtained under statute is to be regarded.

The provision states that:

> "(2) Information shall in any event be treated as obtained fairly if it is obtained from a person who:
>
> (b) is required to supply it by or under any enactment or by any convention or other instrument imposing an international obligation on the United Kingdom;
>
> and in determining whether information was obtained fairly there shall be disregarded any disclosure of the information which is authorised or required by or under any enactment or required by any such convention or other instrument as aforesaid."

Much information which is held by public bodies is supplied by or under an enactment. Individuals have to supply information in a wide range of circumstances, for example in order to apply for planning permission, or to claim housing benefit, or to apply for any one of a number of licences. Because of the interpretation provision such information is always treated as obtained fairly.

For some time I have been considering how this exemption applies if information which is obtained under statute is subsequently to be used for another purpose or other purposes.

Perhaps it may be helpful here to recap on the advice I have given and the general approach I have taken to the requirement that the information to be contained in personal data shall be fairly obtained. My advice to data users has been that

individuals should be informed, at the time the information is obtained, of any data users, uses or disclosures which the individual could not reasonably be expected to anticipate.

Because information which is obtained under statutory powers is deemed to be fairly obtained, the data user obtaining it is not subject to this general rule. However, we live in a world where there is increasing pressure to share information and information is increasingly recognised as a potentially valuable resource. It is possible, therefore, that the data user obtaining the information under statute may envisage using it, not only for the statutory purpose for which it has to be supplied, but for some additional purpose. The data user may also foresee disclosing the information to another body for its use.

It is my view that, in these circumstances, the general rule continues to apply in relation to the other extraneous data users, purposes or disclosures. It is unlikely that the individual supplying the information will anticipate that these additional uses and disclosures will occur and, therefore, the data user should inform him or her of them.

It is not unusual for a data user, when obtaining information for its statutory purpose, to request additional information for administrative convenience or for some other good reason. There is nothing to prevent such additional information being obtained at the same time and on the same form and indeed, in some cases, it will be an efficient way of proceeding. However, the data user should make quite clear which information an individual is required to provide under statute and which he or she is being asked to provide voluntarily.

(e) Lawfulness in the First and Second Data Protection Principles

The First Principle not only refers to fairness but also to lawfulness. It requires that personal data shall be processed lawfully. This term also arises in the Second Principle which requires that personal data shall be "held only for .... lawful purposes".

In dealing with particular data users I have explained my views on the meaning and effect of the term lawful where such questions have arisen. However it is clear that some general guidance is appropriate. The following comments on lawfulness flow from lengthy consideration in my Office, supplemented by advice from leading counsel. The views expressed will have particular significance for the public sector. They will form the basis for a Guidance Note* to be issued later this year.

No interpretation of the term "lawful" is provided in the Act. Therefore, it has to be interpreted in accordance with the normal rule, which is that a word must be given its ordinary meaning unless the context in which it is used shows another intention. There is nothing in the Data Protection Act to suggest that the term should be given other than its normal meaning.

Lawfulness was considered in a House of Lords case in 1991 and in that case "unlawful" was held to mean:

> "... something which is contrary to some law or enactment or is done without lawful justification or excuse."

This is a broad definition; it applies equally to the public and the private sectors and it applies both to those breaches of the law which can be punished by criminal penalties and those which are dealt with by the civil courts.

---

*Guidance notes deal with more specific issues than the Guidelines referred to previously. Details of current guidance notes may be obtained from the Registrar's Office. Copies are provided free of charge.

The effect of this broad definition is that a data user must comply with all relevant rules of law in relation to the purpose for which he holds personal data, and the ways in which he obtains and processes it. So, for example, it seems to me that information which is obtained by theft or in breach of an enforceable contractual agreement is likely to be unlawfully obtained under the First Data Protection Principle. Data users may only lawfully hold personal data for purposes for which they have adequate powers, otherwise the data will be held for unlawful purposes under the Second Data Protection Principle.

Clearly it is not possible to deal with all the different laws that apply to data users and how these interrelate with the Principles. However, there are a number of areas of law which are concerned with the use of information which may have particular significance in relation to the First and Second Principles. These areas of law are ones in which there are current issues or developments. They particularly concern the public sector and government organisations, but may also concern the private sector, for example in relation to financial activities.

Plainly, there are difficult or technical questions of detailed law which cannot be explored fully here and I recognise that some cases may require detailed discussion between particular data users and my Office. However, I hope that the following comments will be helpful and timely. They represent, of course, my view of the law and have not been subject to test by the Courts.

(i) *Confidentiality*

There are circumstances where an obligation of confidence arises between a data user and a data subject. This may flow from a variety of circumstances or in relation to different types of information. Examples might occur in respect of medical information or banking procedures. An obligation of confidence gives the data subject the right not to have his information used for other purposes or disclosed without his permission unless there are other over-riding reasons in the public interest for this to happen.

Where an obligation of confidence arises it is unlawful for a data user to use the information for a purpose other than that for which it was provided. Where such a use involves the processing of the personal data, then this may entail unlawful processing within the meaning of the First Principle. This is important for those who hold and process information which may be subject to an obligation of confidence.

The law of confidence applies to government and statutory organisations just as it applies to private persons. Many such bodies obtain confidential information in order to carry out their duties. An example of this is information which claimants must provide in order to claim some welfare benefits. Claimants may have to provide details of their family circumstances, financial situation and, in the case of some benefits, health information.

However, a wide range of information, not simply that which is clearly sensitive, can be subject to an obligation of confidence. The fact that holding such information carries with it obligations to individuals has been recognised in citizens charter documents which have been produced as a result of recent government initiatives. For example, the Benefit Agency Customer Charter states that the Agency will provide a service which is:

> "Confidential – treating the information you provide in confidence. The information is protected by the Social Security and Data Protection Acts. This means, for example, that you have the right to check information we hold about you on our computers."

I welcome the commitment to the integrity of individuals' information shown by such statements.

Public bodies may obtain much of the information they hold under statutory powers. Such powers are given to these data users specifically to carry out their statutory functions. Where a data user obtains information of a confidential quality in pursuance of its statutory functions and that information is then used or disclosed other than in pursuance of those functions, it is my view that a breach of confidence is likely unless there is some other statutory authority or just cause or excuse for the unauthorised uses and disclosures. If such uses or disclosures entail the processing of the personal data then this is likely to be unlawful processing.

(ii) *The Ultra Vires Rule*

The ultra vires rule does not apply to the Crown. This means that government agencies like the Benefits Agency are not covered by it. The rules applying to Crown organisations are dealt with in the next section. The ultra vires rule is a rule of law which states that those vested with statutory powers are only able to do those things that Parliament has allowed them to do by statute. This includes doing things that are reasonably necessary to allow them to fulfil their primary functions. It follows, therefore, that a statutory body which obtains, processes or holds personal data for a purpose for which it has no statutory authority will be acting ultra vires and therefore unlawfully in holding, obtaining and processing those data.

(iii) *Excess of Delegated Powers*

The rules applying to Crown bodies are similar in effect although technically different in law. Where a particular activity is covered by a statutory scheme, for example the payment of benefits, then the Secretary of State and government agency dealing with that area have to follow the rules laid down in the statute in order to act lawfully. If they do not do so they may be acting unlawfully. Even where there is no detailed specific law dealing with an area and it is dealt with under executive powers then those powers will be defined either expressly or implicitly.

A government body which deals with personal data should therefore ensure it is aware of the relevant statutory scheme governing the activity and the extent of the powers given by the scheme. This is particularly important in so far as there may be specific restrictions on the use or disclosure of data. If the body goes outside the powers to obtain, process or hold personal data it will be doing so unlawfully.

(iv) *The Concept of Legitimate Expectations*

Research carried out by my Office has shown that individuals have varying expectations as to the use, handling and possible disclosure of information provided to public bodies. But there is a continuing, firm, majority belief that government agencies can be trusted to keep and use information in a responsible way. It is within this context of the expectations of individuals that the concepts of legitimate expectation fall to be considered.

In essence this means that in some circumstances an individual who will be adversely affected by a decision of a public body will be entitled to be notified of or consulted about such a decision before it is made. This could apply, for example, if it has been the case that a particular set of information obtained from individuals has not been made public or disclosed and the individual had no reason to think there would be any alteration in this situation. In such circumstances a proposal to disclose this information, where this may have an adverse effect on the individual, may be unacceptable unless the individual has been consulted and given an opportunity to voice his or her position. The individual has a legitimate expectation of consultation which should be respected and complied with. Failure to comply with a legitimate expectation

may render unlawful any holding or processing of personal data associated with the proposed alteration in information practices.

This is a complex area of law where a number of different provisions overlap and interact. Cases will, of course, be considered on their facts,but I shall have the above points in mind when considering whether there have been breaches of the First and Second Data Protection Principles. Such breaches can, of course, give rise to enforcement action to put matters right.

5 Complaints from Individuals

During this year, 4,590 complaints have been received from individuals. This compares with 1,747 such complaints in the previous year. The main reason for this significant increase was a television advertising campaign undertaken in March 1993 (see Section 8). The surge of complaints has created significant staffing problems and at the year end there were 435 complaints awaiting initial assessment.

The advertisement portrayed four examples of the kind of complaint which has been received and investigated. These related to credit reference, vehicle licensing records, criminal records and financial records. The majority of complaints received following the advertisement also related in some way to the example situations.

Of those complaints assessed, 2,628 (63%) were about problems associated with credit reference activities. Many relate to concerns about the extraction of third party information. It, as yet, remains unclear how far the enforcement action which I took (see Section 4(c)) will resolve this type of complaint after 31 July 1993 when new credit reference systems must be installed by the four main agencies. Particular concerns expressed by complainants included the extraction of information about the financial history of every member of the credit applicant's family. The Data Protection Tribunal's decisions in the enforcement actions may not alleviate these concerns.

However, individuals are also questioning the information held by credit reference agencies in other ways. For example, in relation to the length of time for which specific items of data are held and as to whether the data held for the purposes of credit reference are adequate.

Complaints about unsolicited mail have again fallen in number – from 323 in the previous year to 196 in this year. This has been a pattern for the past few years. However, the cases received are raising a greater variety of issues. There have been a number connected with the financial sector, where a customer's personal data may have been passed around a number of companies within the same group to advertise a whole range of financial products.

Of the remaining complaints, 371 (8%) have been about inaccurate data; 338 (8%) about subject access; and 177 (4%) about possible breaches of the First Data Protection Principle, particularly with regard to the fair obtaining of information.

A number of complaints can be dealt with without establishing a detailed investigation. Many of those concerned with the use of third party information in credit reference have, initially at least, been dealt with in this way. However, leaving the television response aside, there has been a trend during the year towards a greater proportion of complaints requiring a detailed investigation. Up until December, some 61% of the complaints received needed to be handled by undertaking such an investigation. However from December the figure has risen to more than 70%. Of the complaints cases closed during the year, 44% were dealt with in under 3 months, 60% in under 6 months and 86% in under one year.

Some particular examples of complaints follow:

Case 1

A man complained that three entries which appeared on his criminal record were not related to him. He believed these convictions related to another person, possibly one who shared his surname. The police force in question advised that the matter had already been resolved through the complainant's Solicitors. However, when the complainant applied for a Hackney Carriage Licence through his local council, a search made of his police record still revealed the same three convictions.

When approached again the police force admitted that its records were still showing this inaccurate information. An investigation by the police force determined that the three disputed entries did in fact relate to another individual, and that his name bore no similarity to that of the complainant. The explanation was that the information had been inadvertently placed on the wrong criminal record. The three convictions were removed from the complainant's record and added to that of the other individual.

Case 2

Several complaints were received from individuals who had seen copies of their credit files showing the numbers of various accounts held by them. In some cases, this had come to light as a result of a relative obtaining a copy of his or her own credit reference file. The complainants were concerned about their financial security when others including employees of organisations who subscribe to the credit reference agencies' systems, gained access to their account numbers.

The main credit reference agencies confirmed that they held account numbers although their practices in respect of them differed. In some cases the account numbers were disclosed to organisations making credit reference checks. However, in most cases this was only done when the account was maintained by the organisation making the check. Account numbers were also supplied in response to a request from an individual, under the Consumer Credit Act, for a copy of his or her credit reference file.

The matter was raised with the Credit Industry Data Protection Forum which includes representatives from the main lender groups and credit reference agencies. The Forum agreed that whilst individuals' account numbers should be retained in order to ensure that received data was attributed to the correct accounts, they should no longer be disclosed to other subscribers or be shown on an individual's credit files.

Case 3

The complainant was telephoned and then visited by individuals who claimed that her vehicle had been in a collision with their's earlier in the day. She showed them her undamaged car and they accepted that she had not been involved in the accident. She was concerned about how they had obtained her name and address. The Driver and Vehicle Licensing Authority confirmed that its driver/vehicle records had not been accessed for this information. As a result an approach was made to the police who confirmed that the complainants details had been obtained through a terminal used by both civilian and police operators. Internal enquiries resulted in a report being made to the Director of Public Prosecutions (DPP). However, the DPP decided that the facts in this case did not justify a criminal prosecution.

Case 4

The complainant had been refused a bank loan and obtained a copy of his credit

reference file. This included an entry relating to a County Court Judgement (CCJ) in his name, and recorded at his previous address. He had lived as a lodger in his sister's home for a year until 1986. However, the judgement, of which he claimed no knowledge, was registered against him at his sister's address in 1989.

The County Court identified the plaintiff for the CCJ as a major water authority. The water authority stated that, although the complainant may have left the address in 1986, they had not received any notification that he, as the account holder, had moved. Therefore, when no payments were made in mid 1989, judgement was entered in his name. The complainant, however, responded that at no time in his year at his sister's address had he ever had responsibility for paying any of the bills, nor did he give his details to the water authority.

On further investigation with the water authority, it appears that when the complainant's sister had contacted the authority by telephone regarding the outstanding bill she had made reference to her "husband". The water authority assumed that her brother was her husband. As a result of this misunderstanding, the water authority agreed to set aside the judgement.

Case 5

The mother of a young student complained that her daughter had received a lengthy personal letter from a prisoner, serving a life sentence for a serious offence, who was completely unknown to her. Whilst at school, the student had attended a computer appreciation course at a local college and it transpired that her lecturer on the course also taught the prisoner who was doing an electronics course.

Early in the computer course the lecturer had instructed the class to type into the computer anything they liked, by way of practice. The student had typed in details of her family, friends and hobbies. The same disk which had been allocated to the student was at a later date given to the prisoner by the lecturer, who was unaware that it contained anything other than technical electronics data. The prisoner accessed the personal data, copied it to another disk and wrote to the student.

It was established that the lecturer cleaned disks immediately when they were required by another class, but if they were not immediately required, they would sometimes be cleaned at a later date. The college had issued advice and instructions to staff and students about data protection requirements, but this incident revealed that the measures it had taken to prevent unauthorised access to data were inadequate.

The college has now put procedures in place with respect to the cleaning and storage of disks which should prevent any recurrence of this sort of incident. These procedures will be embodied in a formal undertaking with my Office which will be agreed with the college.

Case 6

The complainant had been contacted on several occasions over a period of five years by various tracing agencies seeking payment of a long overdue debt owed to a major bank. One of these agencies even approached him through his employer. The complainant had explained on every occasion that he was not responsible for this debt, but that the person who owed the sum had exactly the same name, except for one initial.

In response to enquiries, the bank explained its procedures. It had passed the details of the debtor to the first tracing agent who was unsuccessful in locating him. The bank then employed another tracing agent to pursue the matter, who confirmed

that the debtor did not reside at the address of the complainant. Due to a clerical error, this information was overlooked when another tracing agency was assigned to trace the debtor. This agent was given the complainants' address as the last known address.

The bank explained that the connection had originally been made when the debtor gave his address as that of the complainant. The complainant was sent a letter of apology, and a cheque to cover the costs incurred in attempting to have his name cleared of responsibility for the debt.

Case 7

As a result of being refused credit, the complainant obtained a copy of her credit reference file. This included an entry relating to a County Court Judgement (CCJ) entered against her previous (and her parents' present) address. The CCJ related to a company which she believed was operated by her parents next-door neighbour.

The County Court explained that the address of the defendant had been recorded inaccurately. They provided the address of the plaintiff's solicitors, who were also given details of the complaint. As a result the Court was asked to amend the details of the judgement so that it showed the correct address. It transpired that a typing error had been made by the Court which resulted in the judgement being entered at the wrong address. The complainant was advised to check her credit reference file in a few weeks time to ensure the entry had been deleted.

Case 8

A company ran alarm systems for elderly persons' accommodation. In these systems an alarm is fitted in the dwelling and is connected to a control centre. If a resident activates the alarm, he or she alerts the control room where an operator may speak to the resident or alert some other agency.

In order to respond effectively to alarm calls, the control room staff needed to have access to information about individual residents. This was held both on paper files and on computer. The information was such as to allow staff to make a fast and reasonably well informed decision as to whom they should contact in the event of an emergency. The information included details of the elderly person's medical conditions and other information which might be useful, for example, to a confidence trickster or burglar.

When the company went into liquidation, both paper files and computer files were not properly safeguarded or erased. Print-outs containing details of individual residents were found on the premises after the company had been closed down and the computer was sold with the information still on the hard disk. This case illustrates the necessity for adequate security measures even in small organisations, particularly where sensitive personal information is held.

Case 9

The complaint arose after a summons was incorrectly issued at the complainant's address against an individual with the same name. The summons had been issued by a finance company. The finance company was approached for an explanation of the circumstances leading to the error and for confirmation that the complainant's address had been removed from its records.

It transpired that, when attempting to trace the defendant, inadequate checks had

been made by the tracing agents acting for the finance company. The complainant's address had been obtained, in error, from a telephone directory and no additional cross checks had been made to confirm his identity. The finance company gave assurances that its records and those of its solicitors and tracing agents had since been amended to remove all reference to the complainant's address. The company also confirmed that no information relating to the complainant's address had been passed to any third party organisation.

Case 10

The complainant stated that his previous employers were processing personal data without being registered. It was alleged that the company had been advised several times to submit a data protection registration application but no action had been taken. The complainant sent evidence in the form of waste paper which was taken home by employees to be used as drawing paper for children. Following an investigation, the company was prosecuted and fined.

Case 11

The complaint concerned the layout of VDU terminals in a store. It was claimed that the screens were in such a position that when a customer account card was processed, the details could be seen by anyone else in the vicinity. It was claimed that the information illustrated on the screens was of a sensitive and confidential nature.

An investigation showed that although the terminals were within view of the public, and the screens could be seen from certain angles, no information could be deciphered because of the size of the lettering and the distance of the screens from the public aisle. However, as circumstances might arise where information could be read from the screens, the store decided to fit privacy filters which would limit the viewing of information to the VDU operator.

Case 12

The complainant was unhappy with the way a television rental company had dealt with her direct debit payments. She initially rented several items of equipment from them and paid by two direct debits. In 1991, one of the debits was not drawn upon for six months. The complainant visited her local branch on several occasions and was assured that her account was paid up to date. She then decided to return some of the equipment and to pay for the rest with one direct debit. This seemed to resolve the problem.

In 1992 the complainant received a letter demanding payment of about £200. When this was queried the complainant was told that her bank had requested a refund of this amount and the rental company had been obliged to comply with this request. After further investigation it was discovered that for six months one of the complainant's direct debits had not been drawn from her account, but the money had been taken instead from her ex-husband's bank account. The complainant had been divorced for eight years and had no contact with her ex-husband during that time.

It was discovered that the complainant's ex-husband had changed his bank account from one branch of his bank to another. When this happens it is customary for the new branch to inform all holders of direct debit mandates of this change of branch. In this case the bank had retained an old direct debit mandate dating back eight years and made out to the rental company. Apparently the bank did not notice that this direct debit was dormant and wrote to the rental company informing them of the change of branch. The rental company then amended the bank details held for the complainant.

When the complainant cancelled one of her direct debits, the cancellation was effected against the debit drawn on her ex-husband and no more money was taken from his account. He did not notice that withdrawals had been made until a year later. He instructed the bank to claim the money from the rental company who in turn sought to reclaim it from the complainant.

As the complainant could not pay the full amount at once, but asked to pay by instalments, the rental company registered a default with a credit reference agency.

Following investigation of the complaint,the rental company agreed to remove the default and to update the entry monthly to show only the current amount outstanding. Once the full amount has been paid the account will be shown as having always been up to date.

Case 13

The complainant was a partner in a firm managing a property which was occupied by a caretaker. The complainant himself did not live there or anywhere else in the local authority where the property was located. However, he received a community charge demand as if he did live at the property. On explaining the situation to the local authority he simply received a reminder about the unpaid community charge demand. He then made a subject access request to the authority, but received no reply.

The authority deleted the complainant's details from the community charge register.

Case 14

The complainant had acted as an agent for a catalogue company and encountered problems in collecting payments from one of her customers. When the complainant closed her account she referred the customer's debt to the catalogue company. The complainant had obtained a copy of her credit reference file which showed her account with the catalogue company as being in default.

The catalogue company stated that when agents have such problems with customers the agent is asked to inform the catalogue company and complete a form. Once this is received the customer is transferred from the agent to the catalogue company for the recovery of debt.

In this case the catalogue company had no record of receiving a form from the agent and initially she, and not the customer, had been pursued for the debt. The error was discovered but the complainant's record remained flagged to show her as a defaulting agent.

As a result of the complaint the default flag was removed from the complainant's record.

Case 15

The complainant stated that he made a subject access request to a bank. He alleged that he had not received a copy of the personal data to which he was entitled under the Data Protection Act. Nor had he received a statement to the effect that no data were held concerning him.

The bank was unable to trace a copy of the subject access letter in question

although an entry had been made confirming its receipt. The entry also confirmed that a draft response was processed. The bank admitted its failure to respond to the complainant's request, waived the £10 fee which they usually charged for subject access and supplied the complainant with a copy of his personal data.

The bank stated that all its departments had been advised of the necessity to comply immediately with subject access requests so that there should be no subsequent recurrence of this failure.

Case 16

The complainant stated that when individuals bought goods from a chain store they were asked for their names and addresses so that a company magazine could be sent to them. The complainant said he always refused to give his name because he did not want to receive this magazine.

However, he bought a television set from the store and therefore had to supply his name and address so that this information could be sent to the licensing authority (NTVLRO). He said he had made it clear at the time he had given his name and address that it was only to be used for licensing and that he did not want to receive any mail from the shop at all. He said he was assured that the information would only be used for licensing purposes. He subsequently received a mailing from the store.

The store advised that customers were asked for their names and addresses at the point of purchase. If a customer queried this, then staff explained that the information was used for a mailing list to send a monthly magazine giving details of current promotions. If the customer objected to this, staff were instructed not to persist. Where a name and address had to be given as, for example, in the case of the purchase of a television set, it was the responsibility of the store manager to separate this requirement from that of the mailing list if that was what the customer wanted. In this particular case the store manager had failed to make the separation. However, as a result of the complaint, this customer's name and address was removed from the mailing list.

Case 17

The complainant ordered some goods from a newspaper advertisement and paid for them by credit card. Soon after this purchase the complainant closed his credit card account. Several months after this he received a bill from the credit card company and discovered that it had been presented by the same fulfilment house which had satisfied the order he had made from the newspaper. Further investigation showed that the goods the company said he had ordered had in fact been ordered by his brother who lived in a different part of the country. The complainant's brother confirmed he had made a purchase from the newspaper using his credit card but he had not yet been billed for it. The brothers had a distinctive surname.

The investigation showed that the complainant's brother had telephoned his order to the fulfilment house leaving details on its answering machine. Apparently these details did not include his credit card number. He received a telephone call later asking for this information, which he gave. Somehow his brother's card number was put beside his order and consequently the brother was billed for an order he did not make.

It appeared that the fulfilment house was holding inaccurate data in that the wrong credit card number was held in respect of the second brother's order. The fulfilment house also appeared to be holding personal data for longer than was necessary by keeping the complainant's credit card number after his order had been completed.

The fulfilment house deleted all reference to the wrong credit card number and agreed that when a transaction paid for by a credit card is completed, the credit card number will be deleted. If a refund is requested the customer will have to give his credit card number again.

Case 18

The complainant was in dispute with a mail order company about her account. Although the matter appeared to have been cleared up, the complainant wished to check what information was held about her, and made a subject access request. After 63 days she had still not received a reply.

The mail order company was contacted and it immediately provided the complainant with the information she had requested and an apology.

Case 19

The complainants had taken out an insurance policy, through a large department store, to protect their credit cards and other valuables. Several months later they decided to cancel the policy. The following year they received a notification from the insurance company showing the policy as still open and asking them to update the details. The complainants were concerned that the policy had not been closed and that the confidential information relating to their credit cards and other valuables was being retained.

On examining the department store's application form for the insurance policy it was not clear who was the data user for the information collected on the form – the department store or the insurance company.

The insurance company confirmed that, in normal circumstances, a policy holder's details would be deleted at the time the policy was cancelled. They could not explain why, in the complainants' case, this had not happened. However, as a result of the complaint the policy was cancelled and the data deleted.

It transpired that the insurance company was the data user in respect of the information collected on the application form. It was advised that this should be made clear on the department store's application form. The insurance company administers similar plans for several other organisations and it was pointed out that similar amendments may also be necessary to forms relating to them.

Case 20

A number of complaints were received from customers of two mail order book clubs which were part of one organisation. They had all received invoices for amounts which they did not consider to be outstanding. It transpired that a new computer system had been introduced and a number of accounts had been re-activated in error.

Case 21

The complaint concerned an application form for a store card which included questions asking for the applicant's date of birth and the occupation of the head of household.

It was established that information on the form was sought for two purposes. The first purpose was for the administration of the card; the second for market research.

Some information sought, including that on date of birth and occupation were for the second purpose and failure to provide this information would not affect the store card.

The company was advised to amend its data protection register entry and to re-design the application form to indicate which was for the administration of the card and had to be provided, and which was for market research and need not be provided.

Case 22

The complainant alleged that he had been wrongfully arrested by the police – on two occasions, by two separate forces – as a result of inaccurate data held on the Police National Computer (PNC) Wanted & Missing Persons Index.

Initial discussions with the police showed that the complainant had been arrested on the basis of data, held on the PNC, in connection with a known criminal who shared the complainant's name as an alias.

The police added a rider to the PNC entry relating to the known criminal. This stated that the complainant, known to reside in a given city, was not identical to the wanted man who might use the complainant's name as an alias. This would enable the police to distinguish between the two individuals if the complainant were willing to carry some means of identification at all times.

This action did not seem to provide a satisfactory conclusion, given that the complainant had made allegations that the generation of the supposed alias onto the PNC had been effected in dubious circumstances.

Two police forces continued to maintain data on the PNC relating to the alias name. Neither of these forces had been involved in the alleged wrongful arrests. They were asked if they held any supporting papers which might indicate that the known criminal did indeed use the complainant's name as an alias. Neither had any such papers, and both indicated that they would have 'inherited' the alias details from computer entries, generated by other forces, which had subsequently been removed from the PNC. As a consequence, both forces arranged that all references to the complainant's name be removed from the PNC Wanted & Missing Persons Index.

Case 23

The complainant's credit files showed adverse information relating to an individual who lived in the same road. The complainant lived at number 30 and the other individual at number 22. It transpired that number 22 was originally Plot 30, before the houses were numbered. The financial organisations holding the inaccurate information amended their records.

Case 24

A number of complaints have been received relating to an American publisher. The complainants have been sent an order form inviting them to purchase a book made up of names and addresses of individuals sharing the same surname. The book is designed to appeal to those interested in genealogy and includes the name and address of the complainants themselves. The complainants have generally objected to the inclusion of their details in these publications without their prior consent.

The information is obtained by the company in America from copies of United Kingdom electoral rolls provided by a major British mailing list owner. Although the mailings sent to the complainants had been prepared and posted in America, the UK agent for the company on request, deleted the complainants' details, both from the publication and from its mailing list.

6 Enforcing the Act

It may be helpful to remind readers that enforcement actions can be of two kinds:

— prosecutions for offences flowing, for example, from contraventions of the Act's registration requirements. Most of these cases are triable in either the Magistrates' or Crown Courts, or their equivalent in Scotland and Northern Ireland. They have usually been heard in the Magistrates' Courts.

— supervisory notices, which are designed to set right contraventions of the Data Protection Principles. The Principles set out the good practices with which data users must comply. There are three types of supervisory notice – Enforcement, De-Registration and Transfer Prohibition Notices. The Registrar may also refuse a registration application. These notices may be appealed to the Data Protection Tribunal.

(a) Prosecutions

Charges have been brought this year under the following sections of the Act:

Section 5(1): Holding personal data without being registered or without having applied for registration. (Data users who fail to renew their register entries are also charged under this section.)

Section 5(2)(b): Holding or using personal data for a purpose other than the purpose or purposes described in the register entry.

Section 5(2)(d): Disclosing personal data to a person not described in the register entry.

Section 20: Liability of directors, managers, secretary or similar officer of a body corporate.

Prosecutions have been brought against 68 data users for criminal offences under the Act and a further 10 are awaiting hearing. The concluded cases are listed in Table 1.

The number of prosecutions undertaken this year is virtually double the number reported last year. Since registration, which commenced in 1986, is usually for a period of three years, 1992 was a year in which many data users needed to renew their register entries. I have continued with my policy of prosecuting those data users who should register and fail to do so. This has led to the increase in the prosecution figures. The attitude of the Courts to failure to register under the Act differs greatly as is apparent from the variation in the penalties imposed in non-renewal cases.

I have also had occasion to consider prosecutions under sections 5(2)(b) and (d) of the Act, where data users have acted outside the terms of their register entries. In this respect I have commenced proceedings against two unincorporated associations. Also, for the first time, proceedings have been taken against a company director personally under Section 20 of the Act, since it was his actions which caused the company of which he is a director to act outside the terms of its register entry.

Table 1: Prosecutions in the Year to 31 May 1993

Section of the Act	Data User	Court	Date	Result/Fine £	Costs £
5(1)	F J Griffin*	Kingston upon Thames	01.06.92	Acquittal	Nil
5(1)	Banox Engineers Supplies Ltd	Banbury	05.06.92	Absolute Discharge	125.00
5(1)	Koss Ltd	Marlborough Street	17.06.92	500.00	500.00
5(1)	ECH Project Services Ltd	Clerkenwell	17.06.92	100.00	100.00
5(1)	Tobar Ltd	Swaffham	18.06.92	Absolute Discharge	100.00
5(1)	Norfolk Greenhouses Ltd	Mildenhall	22.06.92	500.00	250.00
5(1)	Reading Football Club plc	Reading	25.06.92	250.00	668.72
5(1)	A C Gordon	Heudon	29.06.92	100.00	100.00
5(1)	Weston Hire (WSM) Ltd	Weston Super Mare	01.07.92	Conditional Discharge	120.00
5(1)	Speed Business Forms Ltd	Peterborough	03.07.92	300.00	250.00
5(1)	Cambridge Recruitment Consultants Ltd	Cambridge	07.07.92	225.00	125.00
5(1)	B S Rowe t/a European House Sales (1985)	East Powder	15.07.92	Absolute Discharge	Nil
5(1)	Carn Brea Leyland Daf Ltd	Camborne	21.07.92	100.00	100.00
5(1)	A Smith t/a Avalon Student Travel	Brighton	22.07.92	150.00	50.00
5(1)	R J Sandrey t/a Swift & Co	Weymouth	07.08.92	150.00	170.00
5(1)	R A O Wolsey	South Ribble	18.08.92	200.00	100.00
5(1)	TGC Computer Products Ltd	Edinburgh	19.08.92	Admonished	Nil
5(1)	S H Potts	Fylde	03.09.92	100.00	100.00
5(1)	P Budd	Bristol	07.09.92	Conditional Discharge	140.00
5(1)	Hampstead Nursing Home Ltd	Hampstead	14.09.92	500.00	200.00
5(1)	Damselstyle Limited t/a Kall Kwikprinting	Richmond-upon -Thames	14.09.92	600.00	539.23
5(1)	Management Week Publishing Ltd	Clerkenwell	17.09.92	Absolute Discharge	Nil
5(1)	S Noble t/a The North of Scotland Commercial Network	Aberdeen	21.09.92	Admonished	Nil

Section of the Act	Data User	Court	Date	Result/Fine £	Costs £
5(1)	I Coates	Conwy and Llandudno	21.09.92	Conditional Discharge	50.00
5(1)	Giga Computers Ltd	Brent	24.09.92	400.00	100.00
5(1)	Jim McColl Associates	Edinburgh	28.09.92	Admonished	Nil
5(1)	K D Goodman t/a Leonard Curtis & Co	Marylebone	16.10.92	200.00	290.00
5(1)	Furlong Bros. (Construction) Ltd	Cheshunt	22.10.92	Acquittal	Nil
5(1)	Solarlux (UK) Ltd	Norwich	22.10.92	200.00	200.00
5(1)	Springcard Ltd	Beverley (Brough)	29.10.92	500.00	150.00
5(1)	J A Gibbs t/a Gibbs Newsagent	Portland	04.11.92	Conditional Discharge	150.00
5(1)	Hockerill Computer Centre Ltd	Bishops Stortford	04.11.92	300.00	706.52
5(1)	J Newman t/a Spadework	Henley-upon-Thames	05.11.92	250.00	450.00
5(1)	Cotton Computers Ltd	Peterborough	06.11.92	Conditional Discharge	230.00
5(1)	Ferguson Snell & Associates Ltd	Brentford	09.11.92	200.00	340.00
5(1)	Landowner Products Ltd	Telford	10.11.92	150.00	25.00
5(1)	Landowner Liquid Fertiliser Ltd	Telford	10.11.92	100.00	25.00
5(1)	Ecowater Systems Ltd	High Wycombe	17.11.92	1500.00	510.00
5(1)	Words For All Reasons Ltd	Wells Street	18.11.92	Conditional Discharge	450.00
5(1)	Dark Horse Communications Ltd	Bromsgrove	20.11.92	250.00	175.00
5(1)	C Addis-Jones	Guildford	23.11.92	Absolute discharge	500.00
5(1)	MPC International (UK) Ltd	Maidenhead	26.11.92	100.00	500.00
5(1)	Evans Glass Company Ltd	Chesterfield	27.11.92	725.00	275.00
5(3)	T J O'Donovan	Vale of Glamorgan	30.11.92	200.00	300.00
5(1)	J H Llewelyn	Vale of Glamorgan	30.11.92	200.00	
5(2)(b)	Chandris Ltd	City of London	02.12.92	Acquittal	Nil
5(1)	Newcastle Mental Health NHS Trust	Newcastle upon Tyne	18.12.92	200.00	382.77
5(1)	Midnight Films Ltd	Marlborough Street	22.12.92	200.00	335.00
5(1)	P & V Redwood t/a Coopers Bailiffs	Redbridge	12.01.93	250.00	250.00

Section of the Act	Data User	Court	Date	Result/Fine £	Costs £
5(1)	Dixon Bale Ltd	Manchester	29.01.93	200.00	200.00
5(1)	Dell Computer Corporation Ltd	Bracknell	02.02.93	1000.00	610.80
5(1)	Mistprestige Ltd	Marlborough	09.02.93	200.00	240.00
5(1)	Philip Wilson Publishers Ltd	Bow Street	15.02.93	350.00	325.00
5(1)	Ocarina Publishing Ltd	City of London	23.02.93	1000.00	325.00
5(1)	N Rigby t/a Visual Eyes	Stockport	24.02.93	280.00	200.00
5(1)	P D Hayter t/a Anchorwatch	Portsmouth	25.02.93	Acquittal	Nil
5(1)	C Whateley t/a Whateleys Newsagent	Huntingdon	01.03.93	Conditional discharge	200.00
5(1)	BPC Underwriting Agencies Ltd	City of London	02.03.93	250.00	500.00
5(2)(d)	Automotive Financial Services Ltd	Worthing	08.03.93	750.00	2250.00
5(1)	Esher Mail Order Ltd t/a Clifford James	Guildford	22.03.93	500.00	812.32
5(1)	P C Jones	Bath	30.03.93	Conditional Discharge	200.00
5(1)	Spring Video Ltd	Ashton-under Lyne	21.04.93 \	2500.00	400.00
5(1)	AMRAF Ltd	Wells Street	26.04.93	250.00	900.00
5(1)	Texas Grills Ltd	South Tameside	17.05.93	400.00	200.00
5(2)(b)	Concorde Chemicals plc	Barnet	19.05.93	450.00 }	1146.05
5(2)(d) S20;	Concorde Chemicals plc	Barnet	19.05.93	750.00 }	
5(2)(b) S20;	T Martell (of Concorde)	Barnet	19.05.93	200.00	Nil
5(2)(d)	T Martell (of Concorde)	Barnet	19.05.93	250.00	Nil
5(1)	Ferguson Oliver Financial Consultants Ltd	Forfar	27.05.93	250.00	Nil

* Appeal (see Section 4)

This year has seen a number of cases brought in the Scottish courts. Prosecutions in Scotland are brought by the Procurators Fiscal and not by my Office. Scottish criminal procedure is different from that in England and Wales and my staff have been greatly assisted in their understanding of the Scottish system by the help of the Crown Office in Edinburgh. The Crown Office has also compiled a document of guidance on the Act which I hope will be finalised shortly and circulated to all Procurators Fiscals to assist and advise them in dealing with cases under the Act.

(b) Supervisory Actions

Enforcement Notices have been served against Trent Mail Order plc and International Correspondence Schools Limited. Both have been appealed to the Data Protection Tribunal and I return to this below.

Preliminary Enforcement Notices have been served against Chartsearch Limited and Linguaphone Institute Limited. They both relate to obtaining information. I serve such notices as a warning of my intention to serve a full enforcement notice. The data user is then given time to respond to this. I have accepted an undertaking from Chartsearch Limited to remedy the situation and am considering representations from Linguaphone Institute Limited.

(c) Appeals to the Data Protection Tribunal

Last year I reported that five appeals were awaiting hearing before the Data Protection Tribunal. Three of those appeals were against refusals of registration. Those three appeals have now been resolved without the need for hearings. In all three cases I had refused to register the data user because the registration application did not comply with the requirements of the Act. Prolonged correspondence had failed to resolve the problem. Before the cases came up for hearing the applicant in each case had remedied the defects in the application to my satisfaction and the cases have been settled by agreement.

The two other appeals which were awaiting hearing were brought by Consumerlink Limited and Innovations (Mail Order) Limited. As noted above, a further two appeals by Trent Mail Order Company plc and International Correspondence Schools Limited have been lodged against enforcement notices I have served this year.

All four of these outstanding appeals relate to the fair obtaining requirement of the First Data Protection Principle in the context of direct marketing. I have taken the view that, to satisfy this requirement, those obtaining information from individuals should explain any data users, uses or disclosures of the information which are not obvious. Such a notification should be given when the information is obtained. Two of the cases are concerned with the subsequent use of personal data which have been obtained without such notification and two relate to the question of the detail and timing of such a notification.

The appeals by Consumerlink Limited, Innovations (Mail Order) Limited and Trent Mail Order Company plc raise similar issues of law. These parties, therefore, asked for their appeals to be heard by the same Tribunal members. There has been a preliminary hearing of the Tribunal in these three cases. This was concerned with the composition of the Tribunal. A full hearing of the cases is expected in September.

(d) Monitoring and Promoting Compliance with the Act

Resources have had to be directed away from the work reported last year on checking compliance with the Act by those obtaining and using information for direct marketing. Also, the "town tests" which were mounted to check and encourage registration in particular areas have been suspended.

The other significant aspect of monitoring and compliance work concerns checking where a data user fails to renew a register entry. To assist data users I have tried to make renewing a register entry as painless as possible. They are sent reminder letters and application forms before an entry expires. If an entry has expired without being renewed further reminders are given and data users are provided with special forms to simplify re-application for registration.

Despite these efforts, a substantial number of data users still fail to renew their register entries. Many have ceased trading; some have been taken over by or have merged with other organisations; some have rationalised their registrations and are covered by another entry. However, there remain those who should have renewed but have failed to do so. In many cases data users do not receive reminder notices because they have moved premises and failed to notify my Office. Where there appears to be such a case new telephone numbers are sought so that the data user can be contacted and sent further sets of re-application forms.

Where there is no response, Investigating Officers visit the data users. This investigatory work has led to the increase in prosecutions this year. Investigations work was halted for a spell late in the year when budgeted funds ran out, however, follow up of those not renewing has now started again and this activity will be stepped up. Those data users who should renew and fail to do so may find themselves before the courts.

(e) Use of a Warrant

In October 1992, the Office was contacted by a County Council Social Services Department. It was alleged that an ex-social worker was holding sensitive data, obtained from employment in the department, on his home computer.

The ex-employee had dealt with adoption and fostering and childcare matters. He had been given permission to use his home computer for his work, but on the clear understanding that all relevant data be handed to the Social Services, should he cease to work for them.

In the light of the information given, and because of the alleged sensitive nature of the data, a warrant of entry was obtained. The ex-employee co-operated with my staff and a computer hard-disk and some 51 floppy-disks were examined. The investigation revealed that no social services data were held. There were relatively minor infringements of the registration requirements of the Act and the ex-employee has been advised to remedy these.

7 The Data Protection Register

Virtually all data users register for three years. They are not able to register for longer periods and registering for one or two years costs no less. The past year has been the one in the three year cycle of register entries which generates the highest number of renewals. The need to renew an entry prompts many data users to amend the details registered in order to bring them up to date. The number of new applications to register has been the highest since 1987, when the first wave of registrations was still being received. During the year, as a result of all these factors, over 35,000 applications to register have been received, together with more than 38,000 requests for amendment and almost 70,000 renewals. At the end of the year there were 166,327 entries on the register.

These numbers make this the busiest year to date for the Registration Department. Unfortunately, this peak workload coincided with a reduction in real terms in the grant-in-aid allocated by the Home Office. Despite cutting back other activities to provide finance for temporary staff and managing a number of system changes to improve throughput, backlogs remain.

A number of temporary staff were employed from September through to March to help with the additional workload. This did enable the department to catch up somewhat in processing new applications and renewal requests, but a disturbing backlog has now built up in these transactions and in processing requests for register amendments. Although steps are being taken to clear this backlog as quickly as possible, it will be some considerable time before processing can be brought up to date. Data users, of course, are not prejudiced legally by this delay since the amendments are deemed to apply, once they are received by my Office, unless and until they are refused.

Despite the high level of activity, the number of register entries which are not renewed when they should be is still causing concern. I refer to this in Section 6(d). The impact of a data user failing to renew is not confined to the Office. It can have a direct effect on other data users in that the level of fee is related to the number of entries maintained on the register.

8 Informing People About the Act

As I explained last year, a cut in the real value of grant-in-aid forced a reduction in sums available for this activity and a re-think of strategy. Costs have been reduced by terminating the contract with the public relations agency and re-organising to establish an in-house Publicity Department. The parting with the agency was entirely amicable and followed a long and helpful relationship. Plans for some extremely limited advertising were changed late in the year when a further £380,000 of grant-in-aid was very helpfully made available for this purpose by the Home Office. The results of this are explained below and in Section 9. Statistics on awareness activities to date are given in Appendix 5

I remain convinced of the importance of educating both the public and data users on data protection and am grateful for the additional support the Home Office provided. However, in the present public expenditure climate, it would be foolish to expect such additional funding to recur. The strategy outlined last year will therefore continue to be developed. This comprises concentration on pro-active public relations work; provision of information, advice and educational materials; and more regular contact with and support for trade and other representative bodies, libraries, citizen's advice bureaux, schools and colleges.

Publicity is, of course, a two-edged sword as far as resources are concerned. I refer in Section 5 to the problem of handling the complaints received as a result of the television advertising campaign. It is also worth noting that a small editorial piece in the Daily Mail yielded more than 500 requests for information over a few days. Success also has the seeds of potential disaster in a time of constrained finances and many competing demands for resources.

(a) Advertising

The additional grant from the Home Office largely financed a good medium-weight television advertising campaign throughout the month of March on Channel 4 in Scotland, the Midlands and North of England and on satellite TV.

The campaign was directed towards informing individuals of their rights under the Act and utilised the commercial made in 1990 ("There must be some mistake!"), edited down to 30 seconds. Viewers were invited to write for further information to a freepost address. The commercial was clearly seen by viewers principally as an invitation to write to the Registrar about their problems. More than 3,600 responses were received, of which some 70% were complaints about perceived misuse of personal data. All responses were dealt with in-house.

The principal purpose of the advertising, however, was not to obtain the maximum response, but to convey the message that individuals are able to do something if mistakes are made on computer. Research carried out after the advertising (see Section 9) suggests that the campaign may have got this message over to another 1,250,000 adults in the campaign region.

(b) Public Relations

As the new publicity department was not operational until December 1992, its full effect has not yet been realised. However, throughout the year 19 press releases were issued, over 1,000 press mentions recorded and staff gave 14 radio interviews. The rate of activity increased in the early part of 1993. During this period journalists were reminded of our remit and of current data protection issues through a supplement to the UK Press Gazette.

Databases of those wishing to be kept informed of new data protection developments or publications, and of interested journalists have been set up so that they can be sent appropriate mailings.

(c) Publications

In November 1992 all registered data users and computer bureaux were sent a new edition of the Data Protection 'Update' newsletter. The newsletter was accompanied by a year-planner which listed the Data Protection Principles. An offer of additional copies of this year-planner was well received and some 148,000 have been distributed in total.

As part of a policy of tailoring literature for specific markets, a new information pack "Dealing with the Data Protection Act – A Guide for Small Businesses" was printed in April. This is being made available through small business organisations and advisers.

The demand for printed material has continued to grow. Throughout the past year, the Office has distributed over 80,000 copies of the introductory leaflet "What is Data Protection?", 34,000 sets of the eight Guideline booklets, and 30,000 copies of the individual's rights leaflet "If there's a mistake on computer about you". Also, 48,000 registration packs have been provided, in addition to 35,000 special registration packs for schools.

More than 3,000 copies of the new fifteen-minute introductory video ("What is Data Protection?") have been distributed during the year, largely in response to requests from existing registered data users and representative bodies. Throughout the coming year, further work will be undertaken on distributing the video to organisations such as libraries, small business advisory centres, and personnel and training managers.

(d) Policy Work

Much information on the Act is of course given by policy staff in their discussions with representative bodies and through advice to particular data users. This activity was supported by around 100 presentations at seminars and conferences to a wide variety of audiences.

(e) Other Activities

As an experimental exercise, the Office mounted a series of free one-day introductory seminars on data protection in the early part of 1993. In March, seminars were held in Liverpool, Manchester, Sheffield, London, Bristol and Cardiff. In June, the seminar was held twice in London, and in Birmingham, Glasgow and Edinburgh. At the same time, two specialist seminars were also held in London for the Public Sector and the Financial Sector. All the seminars were over-subscribed, with some 3,500 enquiries being received and 1,100 people actually

attending. Later in the coming year, this activity will be reviewed in the light of available resources.

The Office took stands at only 7 exhibitions throughout the year, a reduction in relation to previous years which resulted largely from budgetary constraints. 'Town Tests', where publicity and investigational work is concentrated for a short period on a single town, were also suspended due to lack of funds.

Last year was the busiest year for the Enquiry Service since the initial registration year of 1985/86. This year has been even busier and staff have dealt with 43,495 telephone calls and 15,818 letters.

9 Background Research

Once again this year research into awareness of the Act was carried out amongst both the general public and data users, large and small. Detailed results from this year's survey are included in Appendix 6 together with comparative figures from the two previous years.

In order to assess the effect of the television advertising campaign in March (see Section 8), a further more limited piece of public awareness research was conducted in April. Some conclusions from this are referred to below.

(a) Public Attitudes and Awareness

The first main piece of research revealed that overall awareness and knowledge of the Data Protection Act had stayed much the same amongst the general public. Around one in 5 people are aware that there is a law about information kept on individuals and about half of these make spontaneous mention of the Data Protection Act. Prompted awareness of the Act and the Registrar remains at about 50% of the general public.

This year there has been some decline in the perceived importance of a number of issues. This may be because the 1992 research, which produced unusually high figures, was conducted during the general election campaign. The fall in respect of the number of people who regard protecting peoples' rights to personal privacy as very important (from 78% in 1992 to 66% in 1993) is shared with: preventing crime on the streets (91% to 85%); inflation (66% to 46%); and protecting freedom of speech (67% to 53%).

The research carried out following the March 1993 TV advertising campaign showed that although awareness of "data protection" in terms of awareness of the Data Protection Act or the Data Protection Registrar had not increased, there was an increase in awareness of related concerns. For example in the television areas targeted, the proportion agreeing strongly that "something can be done if mistakes are made on computer" increased from 34% before the campaign to 41% afterwards. The rise in agreement with the proposition that there is "somebody who can advise me about getting computer mistakes put right" was from 61% to 69%.

(b) Data User Awareness

The data user research distinguishes small users (organisations with fewer than 50 employees) from large users (those with 50 employees or more).

The proportion of small data users holding personal records on computer has grown from 46% to 51%. Prompted awareness of the Data Protection Act amongst these organisations remains high at 87%. However, awareness of the need to register and of other obligations flowing from the Act have also remained the same at 59% and 29% respectively.

All large companies surveyed used computers and held personal records on them.

Here, prompted awareness of the Data Protection Act was virtually complete at 97%. Awareness of the need to register held firm at 85% and awareness of other obligations rose from 45% to 56%.

When considering these figures, it is worth bearing in mind that the respondents to the surveys, more particularly in the larger organisations, may not have any direct responsibility for data protection or matters of data protection importance. The fact that not all large organisations appear to know about registration does not mean that they are not actually registered.

10 International Activities Outside The European Community

(a) The Council of Europe

My staff attend the meetings of the Council of Europe Project Group on Data Protection and the Working Group on Medical Data.

The Committee of Ministers has considered the recommendation on the protection of personal data in telecommunications, but has referred this to the Steering Committee on Human Rights. Approval of the recommendation cannot now be expected before September 1993.

The Working Group on Medical Data held its final meeting in July 1992. Its recommendation has been revised by the steering committee (Bureau) of the Project Group and now includes safeguards in respect of genetic data. The recommendation is expected to replace the existing recommendation on medical databanks dating from 1981.

The Committee of Ministers has asked for an evaluation of the recommendation relating to the use of personal data in the police sector and of the need to revise this.

Deliberations continue on data protection in respect of census and statistical data and written comments on a draft recommendation are to be submitted by August 1993.

(b) The International Conference of Data Protection and Privacy Commissioners

The 1992 meeting took place in Sydney, the first time that it has been held in the southern hemisphere. Discussion covered a wide range of topics, notably issues relating to employment, telecommunications and medical data. I look forward to hosting the fifteenth such meeting in Manchester between 27 and 30 September this year.

The Working Party on Telecommunications has met twice in the year, in Berlin and in Moscow. It produced a report for the International Conference of Data Protection and Privacy Commissioners drawing attention to areas of concern relating to the security of telecommunications and satellite communications. It has also considered other issues including credit cards and security of mobile telephones.

(c) Other International Contacts

One of my staff attended the OECD Ad Hoc Experts Meeting on Data Privacy Protection held in Paris. My Legal Adviser gave a keynote address to the Third Conference on Computers, Freedom and Privacy in San Francisco in March and one of the Assistant Registrars presented a paper at the Conference in Warsaw of the

Universal Federation of Travel Agents.

Two meetings of the British Data Protection Authorities took place; in Jersey and Guernsey.

My Office has this year received visitors and delegations from Australia, Belgium, Canada, France, Hong Kong, Japan, New Zealand and Romania.

There have been useful exchanges of information with a number of other countries. In particular, two of my staff made a short visit to Germany for discussions at both Federal and Land level with those responsible for data protection. Also, I was pleased to welcome members of the Commission Nationale de l'Informatique et des Libertés (CNIL), the French data protection authority, to Wilmslow for two days of very useful and interesting discussions. I record my gratitude to these Authorities, and to those of other countries, for their co-operation and assistance over the past year.

11 Organisation and Finance

(a) Level of Grant-in-Aid

The 1992-93 financial year saw a reduction in initial grant-in-aid of 6.2% in real terms. The subsequent allocation of a further £380,000 by the Home Office late in the financial year was most welcome. As explained in Section 8, these additional funds financed an advertising campaign designed to inform members of the public of their rights.

The grant-in-aid for 1993-94 amounts to a 1.9% reduction in real terms as compared with the original grant for 1992-93. This makes for a further difficult year, particularly in the light of the substantial increase in the number of complaints noted in Section 5.

However, it is the prospect for the financial year 1994-95 which gives me the most concern. It is clear that there is becoming little point in calculating and bidding for what seems to be appropriate and necessary finance for the tasks ahead. In requesting forecasts for 1994-95 the Home Office has asked for information as to the effects of a 10% reduction from the grant allocated for 1993-94. Any reduction would compound present difficulties and I have advised that a reduction of 10% would leave the Registrar unable to carry out his statutory duties and open to actions for judicial review.

An organisation can be in a state of development, maturity or decline. This state will strongly influence the feasibility of cutting back finances without severe damage to that organisation's role and objectives. The worst damage will occur when the organisation is still in a state of development, particularly if that development is driven by demands which are legitimate, but outside the organisation's control. This Office is in that worst case position.

The feasibility of cutting back expenditures without damage is also dependent on how efficiently an organisation is meeting its prescribed tasks. Two independent reviews – a Staff Inspection in 1987 and a Financial Management Review in 1990 – have both concluded that this Office is tightly complemented, well organised and monitors and uses its resources effectively. Despite this, efforts have continued to find better ways of doing things, to improve productivity and to reduce expenditures. The possibilty of achieving such improvements and savings inevitably becomes less and less.

(b) Raising Revenue

Revenue raised by the Office is paid to the Home Office for appropriation to the Consolidated Fund. It has no bearing on the year on year grant-in-aid made available to the Registrar.

Nevertheless, it has seemed appropriate for the Registrar, at times, to make charges for services provided. With this in mind, I have taken legal advice on whether I have the statutory power to make such charges. The conclusion is that I do not and that there is no proper method by which I could make charges or establish

arrangements for charges to be made on my behalf. This is a point which should be considered in any future revision of the Act.

(c) Results for the Year

Expenditure for the year was £3,723,455. Receipts from Registration fees amounted to £7,726,669. Registration fees were particularly high because, as described in Section 7, 1992-93 was a peak year for registration renewals. In addition a further £115,377 was received from a variety of sources including interest earned on funds temporarily invested during the year.

The Statement of Account for the year ended 31 March 1993, as certified by the Comptroller and Auditor General is in Appendix 7. I am grateful to the National Audit Office for processing the audit rapidly so that the final account could be included with this report.

12 Conclusions

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. The current draft of the directive is founded on a right of privacy which will take its place alongside any developments from current considerations on privacy and the media. The draft sets a balance of interests which, in comparison with the present Data Protection Act, tilts towards greater protection for individuals. That seems appropriate in the light of the developing collection and use of personal data. This report shows that such developments continue apace in both the public and private sectors.

Administration of the Act touches on very many activities. As might be expected this reveals not only the value of the Act but where its boundaries of influence lie. An example of this arises in connection with the possibility, referred to in Section 3, that there may be a market in personal data in operation. Here, I conclude that the position in law governing unauthorised access to personal data, for example by enquiry agents, may merit further consideration by Ministers and Parliament.

The determination of the meaning of the Act lies initially with the Registrar and subsequently, on appeal, with the Data Protection Tribunal and the Courts. During this year the first two appeals have been heard before the Higher Courts, one taken by my Office and one concerned with a prosecution undertaken by the Director of Public Prosecutions. The details are in Section 4, but I was particularly interested to see that the Court of Appeal, in the second case, took the view that the purpose of the Act was to protect the interests of private individuals. This supports the view previously given by the Data Protection Tribunal that in assessing "fairness", the most important single consideration is the interest of the individual data subject.

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 of close to 29,000 a year. This peak rate, of course, only lasted for a few weeks. However, it is clear that there are latent problems to be addressed and complaints are still being received at a rate well over the previous level.

Overall awareness of the Act and the Registrar have not changed over the year. Prompted awareness of data protection remains at about 50% of the population. This figure gives an idea of year on year changes but it is difficult to be clear what it means in effect when a particular individual has a problem. There was a significant increase in awareness, in the areas where the television campaign was held, that help was available to put computer mistakes right. However, those who are aware, without prompting, that there is a law concerning rights about information kept on individuals remain at 20% of the population. Clearly it would be valuable to raise this figure, but it is difficult to be sure how feasible this is, or whether the figure is good, bad or indifferent, without comparable figures for other legislation. Effort will continue to be directed to "grass roots" activities of raising awareness through providing advice and materials for schools and other educational establishments. It seems unlikely that funds will be available for further advertising on any scale.

Last year proved difficult in financial terms. A real reduction in grant-in-aid

coincided with a peak registration year and the effects of that are still being felt. The surge of complaints has made it necessary to halt some activities and transfer resources from others. The number of staff available for policy work in connection with the police, health, financial sector and other matters outlined in Section 3 has had to be cut back. This difficult situation will continue in 1993/94, but in this respect, the Office is in no different position to many other public sector organisations. However the subsequent year gives rise to the most concern. A further reduction in the grant-in-aid in 1994-95 raises the spectre, for a new Registrar, of an Office unable to carry out its statutory duties and subject to the possibility of judicial review.

Much remains to be done. The future holds interesting changes, many challenges and an underlying financial threat to progress with the tasks in hand.

E.J. HOWE
DATA PROTECTION REGISTRAR
JUNE 1993

Appendix 1

Commission of the European Communities Revised Proposal for a Council General Directive on Data Protection

A Commentary by the UK Data Protection Registrar

Note: In this paper, except at the first time of mention:

— the Commission of the European Communities is referred to as "the Commission";

— the revised draft directive on data protection is referred to as "the revised draft";

— the original draft directive on data protection[2] is referred to as "the original draft";

— the Council of Europe Convention on Data Protection[3] is referred to as "the Convention";

— the United Kingdom Data Protection Act 1984 is referred to as "the Act".

1. INTRODUCTION

1.1 In 1990, the Commission of the European Communities published a package of proposals on data protection. This package contained the original draft of the general directive. Following consideration and comment by the European Parliament a revised draft of this directive is about to be published by the Commission. This paper considers that revised draft.

1.2 The Commission's initiative is welcome. Establishing rules about the lawfulness of processing, emphasising particularly the consent of the data subject, and the granting of specific rights to individuals would enhance the protection of individuals in the United Kingdom. The revised draft does, however, present a number of practical problems.

1.3 This paper considers whether a European Community Directive on Data Protection is needed. It then describes the principal objectives of the revised draft and picks out some issues of principle for consideration. Finally, it gives more detailed comments on specific articles in the directive before a brief conclusion.

2. DO WE NEED A EUROPEAN COMMUNITY DIRECTIVE ON DATA PROTECTION?

2.1 The Council of Europe Convention (Treaty 108) on Data Protection was

1. Proposal for a Council Directive concerning the protection of individuals in relation to the processing of personal data (COM (92)422 final – SYN 287).
2. Proposal for a Council Directive concerning the protection of individuals in relation to the processing of personal data (COM(90)314 final – SYN 287).
3. Convention for the protection of individuals with regard to automatic processing of personal data (European Treaty Series, No. 108). Opened for signature in Strasbourg on 28 January 1981

opened for signature in 1981. The Convention seeks to establish a set of individual rights and a standard for handling information about individuals. The objective is to achieve a level of protection for personal data within different nations such that personal data may flow freely between them. Thus, the Convention supports the free flow of information conducive to beneficial administrative and commercial activities where there is proper regard for the position of individuals.

2.2 A number of European countries have introduced data protection laws to allow them to ratify this Convention. Ratification by European Communities (EC) Member States has been encouraged by resolutions of the European Parliament, recommendations of the Council of Ministers and Commission initiatives. Despite this, Italy, Belgium, Greece and Spain have still not passed data protection legislation enabling them to ratify the Convention, although Spain has ratified in the absence of legislation. Italy and Belgium are actively pursuing legislation.

2.3 Even those countries which do have legislation, have legislated in distinctly different ways. The issue of whether one country gives protection equivalent to another has caused some difficulty. Moreover, some data protection authorities may stop the transfer of data to a country which has data protection legislation and which has ratified the Convention but which, in a particular case, does not have the protection afforded by the law of the transmitting state.

2.4 There are other practical problems arising from the multi-national nature of some data processing operations. A parent company which arranges to process the data collected by its various European subsidiaries at a bureau in the United Kingdom may be quite uncertain which data protection laws it must satisfy and there is always a risk that the requirements of those laws will be inconsistent.

2.5 The Single European Act adopted in Luxembourg on the 17 February 1986 introduced procedures to ensure the establishment of the internal market in the European Community by 31 December 1992. Article 8A of the Treaty of Rome defines the internal market as an area "without internal frontiers in which the free movement of goods, persons, services and capital is ensured in accordance with the provisions of this Treaty". With the advent of the single market, then a single regime for data protection acceptable to all Member States would seem to be not only unavoidable but also desirable. Without the free flow of personal data between Member States there is a clear danger that the other free movements that the Single European Act requires will be undermined. There would seem, therefore, to be a need for a directive, however, the question remains open as to its scope and nature.

3. Principal Objectives of the Revised Draft

3.1 The first objective is to harmonise data protection laws in the Member States. The intention is to harmonise at a high level of protection for individuals and not to prejudice any protection given already by the legislation of individual member states. This approach has been adopted partly by analogy to the requirements of paragraph 3 of Article 100A of the Treaty of Rome which requires consumer protection legislation to be harmonised at a high level and partly because some states see data protection as an example of the human rights currently protected by entrenched provisions of their constitutions.

3.2 The parallel objective of the revised draft is to create an area within which personal data can be transferred without restriction. That is achieved by Article 1(2) which bans the prohibition or restriction of the flow of personal data between member states on data protection grounds.

4. Some Issues of Principle

4.1 *A Right to Privacy:* The revised draft emphasises in Article 1(1) that its subject matter is the protection of:

> "The rights and freedoms of natural persons with respect to the processing of personal data, and in particular their right to privacy"

This is a clear, welcome, statement that data protection is a human rights matter rather than any question of the technical regulation of computers. Would this Article put beyond dispute the question of whether any privacy right existed in United Kingdom law?

4.2 *Balancing Rights:* Nevertheless, data protection has to be about balancing rights. The Convention is quite clear that data protection is a restriction on the rights of individuals to hold and transmit information and can only be justified so far as is necessary to secure the proper protection of privacy. In other words, a balance has to be struck between Articles 8 and 10 of the European Convention on Human Rights (European Treaty Series No. 5).

4.3 The Data Protection Act 1984 seeks to comply with the Convention and, therefore, reflect the balance which it strikes. The revised draft supplements the general rules of the Convention with some specific provisions, particularly in the matter of sensitive data, the need for the consent of the individual and rules on the legitimacy of processing. These may shift the balance somewhat in favour of the individual as compared with the Act. Whilst detailed criticisms can be made of some of the provisions, this new balance does not seem unfair.

4.4 *Consent:* The revised draft expressly introduces a requirement for the consent of individuals to the processing of personal data in certain cases. This is particularly so where data, such as health records, is defined as "sensitive". This is a distinct difference from the Act. Some countries have followed Germany in seeking to expound the right of 'informational self-determination'. It is not necessary to accept that view of individual rights in order to conclude that the requirement for consent might be appropriate and valuable in certain cases.

4.5 On the other hand, the revised draft sets out rules which, if followed, should legitimise the collection and processing of personal data in most cases, without the need to gain the consent of the individuals concerned.

4.6 *Manual Records:* There has been a debate about extending data protection to manual records. It is said that no difference in principle can be seen between the risks to individuals created by manual and automated records. Consequently, the same protection should be extended to individuals in relation to both types of information storage.

4.7 On the other hand, the Convention and other international instruments were expressly justified on the basis that the power of automatic processing to assemble, rearrange, manipulate and communicate data posed such a significant potential threat that special legal protection was required to protect the privacy of individuals. It is not clear that traditional manual processing poses the same quality of threat to individuals as automated processing; this issue is considered again at section 5.5 of this paper.

5. Detailed Comments on the Revised Draft

5.1 A New Approach to Data Protection Rules (Chapter II)

5.1.1 The original draft set out detailed rules about the lawfulness of the collection, processing and disclosure of personal data. It then independently

incorporated the more general rules on these matters found in the Quality of Data provisions in Article 5 of the Convention. The relationship between the general rules and the specific was unclear. In addition, rules for the public and private sectors differed.

5.1.2 The wholesale recasting to be found in Chapter 2 of the revised draft is to be welcomed. The Chapter now leads with the general Quality of Data provisions in Article 6 and thus gives them the prominence they merit. In the process of recasting, the distinction between public and private sectors has been largely dispensed with. This also is welcomed. There remains a problem as to how some of the more detailed rules, which now follow in the text, are to be subordinated to the general requirements.

5.2 Registration (Articles 18-21)

5.2.1 A registration system is central to the Act. Registration makes for openness on the part of those processing personal data. It can also be used to regulate undesirable processing. Under the United Kingdom Law, exemption from registration is effectively exemption from data protection control.

5.2.2 The original draft proposed a comprehensive scheme of registration (called 'notification' in the directive). There is now a helpful relaxation of that scheme. The inclusion of extensive exemption and simplification procedures will aid concentration on matters of greater, rather than lesser data protection significance. It is important to note that exemption from notification would not release data users (controllers of data in the directive) from the duty of complying with substantive data protection rules.

5.3 Subject Access (Articles 13 and 14)

5.3.1 The right of an individual to obtain information about him or herself (subject access) is fundamental to data protection objectives. There have to be exemptions such as those permitted by the Convention for national security, defence, criminal investigation and certain other cases, but they have to be restricted to those constituting 'a necessary measure in a democratic society'.

5.3.2 The revised draft has a welcome extension of subject access exemptions to the private sector. There seems to be no reason of principle why they should not so apply if justifiable on their merits.

5.3.3 It is regrettable that the Commission has not provided for an exemption from subject access to protect the data subject (an individual) him or herself. Such an exemption is permitted by the Convention and needs to be relied on to justify withholding information in a case, for example, where giving it to a medical patient may cause serious harm to the patient. Such cases may be rare, but they should be provided for and it is not satisfactory to say that the specific medical case can be dealt with by indirect access to the data through another medical practitioner.

5.3.4 Individuals are given an important extra right to refuse to exercise their subject access rights under the compulsion of a third party. This is a specific United Kingdom problem, where, for example, prospective employers have required applicants to exercise subject access rights in order to vet their criminal records. The proposal in the revised draft is a step forward but it might be preferable to prohibit a third party from making such a demand rather than merely granting the right to the individual to resist it.

5.3.5 The revised draft has, however, raised another anxiety. Article 14 now opens with the expression:

> "Unless obliged to do so by a provision of Community Law, Member States may by law restrict the exercise of (subject access rights)..."

The implication is that there are, or will be, provisions of Community Law depriving individuals of the right of subject access. It is believed that this refers especially to the Money Laundering Directive approved by the Council of Ministers on 10 June 1991, Article 8 of which runs as follows:

> "Credit and Financial Institutions and their directors and employees shall not disclose to the customer concerned nor to other third persons that information has been transmitted to the authorities in accordance with Articles 6 and 7 or that a money laundering investigation is being carried out."

5.3.6 Article 6 requires Credit and Financial Institutions to inform authorities of any fact which might be an indication of money laundering and to furnish information to the authorities on request. Article 7 restrains Credit and Financial Institutions from carrying out suspect transactions until they have notified the authorities. "Third Parties" does not seem to be defined in the Directive. "Authorities" is not defined as such but is presumably to be taken as a reference to "the authorities responsible for combating money laundering of the Member State in whose territory the institution forwarding the information is situated", as referred to in Article 6.

5.3.7 On the face of it Article 8 imposes a strict blanket prohibition on giving specified information to a customer or anyone other than the defined authorities. Presumably the prohibition applies to data protection authorities and even the Courts. It is a matter of concern that the Data Protection Registrar might be prevented from inspecting records containing information of this nature. Moreover, the prohibition on giving information to a customer goes much further than the subject access exemption contained in Section 28 (1) of the Act.

5.3.8 The Act contains a balancing provision by which information can only be withheld from a data subject if to provide it would be likely to prejudice the prevention or detection of crime, the apprehension or prosecution of offenders, or the assessment or collection of any tax or duty. A balanced exemption such as that can be justified as a derogation under Article 9 of the Convention on the grounds that it is, "a necessary measure in a democratic society in the interests of ... the suppression of criminal offences". It is not at all clear why it was thought necessary in the specific case of money laundering to impose a blanket prohibition without any such test as is found in the United Kingdom legislation. The prohibition overrides the right of subject access even when it is clear that the information would be given to an entirely innocent customer of a bank.

5.4 Transborder Data Flow Control (Articles 26 and 27)

5.4.1 If there is to be a Community with an acceptable and high level of individual data protection, which thereby permits the unrestricted transfer of personal data throughout the Community, then it is to be expected that there will be a fence around the Community with some means of guarding it. Transborder data flow controls are to be expected and are legitimate.

5.4.2 Under the original draft, transfers of personal data either temporary or permanent to non-EC countries might only take place if an adequate level of protection were ensured (Article 24.1). Member countries had to inform the Commission of cases in which there would not be adequate protection. The Commission might negotiate with third party countries on behalf of the Community and might prescribe a list of countries which ensured adequate protection. Member States might permit transfers in breach of Article 24.1 in particular cases, after informing the Commission and Member States and not having received notice of opposition within 10 days. In a disputed case, the Commission were to adopt unspecified appropriate measures.

5.4.3 It was not clear how this would operate in practice and whether it implied an overly-bureaucratic licensing process for individual data flows. The revised draft seeks to address that problem by adding, to the new Article 26, substantial exemptions permitting transborder flows in order to enter into or fulfil contracts, with the consent of the data subject and on certain other grounds.

5.4.4 The revised draft also seeks to guide the assessment of the adequacy of protection in a third country. The individual case is to be examined and soft law – such as professional rules of conduct – may be taken into account. The original draft was criticised by some for using the expression 'adequate protection' rather than the phrase, drawn from the Convention, 'equivalent protection'. If the European Community nations are to have equivalent protection for personal data crossing internal boundaries, it does not seem unreasonable to look for this standard in other countries, albeit ways of achieving it may differ.

5.4.5 This issue is complex. Transborder data flow provisions have considerable implications for relations between the EC and non-EC European countries. These include those countries which, rather than ratifying the Convention, aim to follow the similar rules in the OECD guidelines, but which do not have private sector data protection legislation on European lines. Most prominent amongst these countries is the United States of America. The Commission has had to try to achieve a protected data protection community, whilst not unreasonably disrupting legitimate and important trade links. Providing that positive action is taken to achieve common standards and to tackle problems which arise, and, notwithstanding some anxiety about the provisions, the revised draft adds a degree of useful flexibility and is an improvement on the original.

5.5 Manual Records

5.5.1 There are reasons both of practicality and principle for avoiding comprehensive regulation of manual records. On the other hand, there are occasions where regulation might be justified. It would be valuable for data protection legislation to apply to those cases where a system has been partly automated and there seems to be an arbitrary stop to the jurisdiction of the Registrar when investigating complaints. In cases of particularly sensitive data or sensitive uses of data, some control might be appropriate and in particular perhaps there should be a right of subject access.

5.5.2 However, there can be difficulty in applying traditional data protection principles such as accuracy, adequacy and relevance to manual source documents particularly if they consist of correspondence addressed to an organisation unbidden. There is also a need to be cautious that there are not excessive restrictions on the rights to freedom of expression recognised by Article 10 of the European Human Rights Convention.

5.5.3 The Commission has sought to recognise these difficulties by restricting the class of manual records covered by the proposal to those within Article 2(c). The definition of 'personal data file' found here is a major revision of the original draft. It seems to be seeking to cover principally summary records, extracted from primary sources, which can be searched in order to find out something about, or to classify an individual. Whilst there can be sympathy with this aim, it is difficult to be confident that the proposal is yet framed in a clear enough way to achieve the proper balance between the various considerations touched on.

5.6 Sensitive Data (Article 8)

5.6.1 The directive extends the class of specially sensitive data found in the Convention by adding trade union membership.

5.6.2 The Convention, whilst recognising that certain data are generally sensitive requires only that their processing should have appropriate safeguards.The

major difficulty in the revised draft is that it starts with an absolute prohibition on processing sensitive data. That would apply to data of a routine nature such as an employer's sickness absence records and could cause particular difficulty because a person's name alone can reveal racial or ethnic origin and perhaps religious beliefs.

5.6.3 Objection could be taken to this prohibition as a matter of principle. The Commission has sought to recognise practicalities by substantial exemptions and, in particular, the new Article 8(2)(c) which authorises processing "where there is manifestly no infringement of privacy or fundamental freedoms". Article 8(3) permits processing in certain cases, subject to safeguards, even where there would be such an infringement.

5.6.4 Article 8(4) deals specifically with criminal convictions. In the original draft, this provision was heavily criticised for apparently preventing an employer from keeping a note of his employees' work-related convictions. There is now considerable scope for Member States to provide legislative authority for the keeping of these records.

5.7 Media Exemption (Article 9)

5.7.1 There are no exemptions from the Act for the media or journalists. Whereas the matter might at one time have been largely academic, the use of highly automated systems, both in the press and broadcast media raises issues of policy and practicability.

5.7.2 The original draft at Article 19, gave Member States an option to grant exemptions to the media as follows:

> "The Member States may grant, in respect of the press and the audio-visual media, derogations from the provisions of this Directive in so far as they are necessary to reconcile the right to privacy with the rules governing freedom of information and of the press."

5.7.3 The revised draft contains an article which will compel Member States to grant exemptions for the media from data protection laws thus:

> "To reconcile the right to privacy with rules governing freedom of expression, Member States shall prescribe exemptions from this Directive in respect of the processing of personal data solely for journalistic purposes by the press, the audio-visual media and by journalists."

The revised article sets the objective of the exemptions as (and probably restricts them):-

> "to reconcile the right to privacy with rules governing freedom of expression, ..."

The whole article is founded on the footing that there is a right to privacy.

The press has a very important role in a democratic society. However, the right to grant exemptions should not be interpreted so widely as to unduly prejudice the protection of privacy which the directive seeks. If subject access exemptions were specifically granted to investigative journalists, for example, it would be difficult to understand why these should be wider than those available to the police. It would be helpful if it were made clear that exemptions under Article 9 could be granted only so far as is strictly necessary to reconcile privacy rights with the freedom of the press.

5.8 Fair Obtaining of Information (Articles 6(1)(a) & 11)

5.8.1 The requirement in the Act that information shall be obtained fairly has

proved to be of particular practical importance. It is reflected in Article 6(1)(a) of the revised draft (it should be borne in mind that processing has been defined in the text to include collection as distinct from the more usual definitions in the Convention and the UK legislation).

5.8.2 The Registrar's view of fair obtaining is that when information is sought, if it is not obvious to the source who you are, what you will do with the information and to whom you will give it, then those matters should be explained. It may be that this duty of fairness is owed to the data subject as well as the source where they are not the same.

5.8.3 Article 11 of the revised draft specifies, in some detail, the information which must be provided to an individual when data are collected. The original draft largely reflected the Registrar's view of what should be done in the typical case, but it seemed to be too inflexible, especially because information had to be given to an individual where it was obvious or had been given previously.

5.8.4 Possibly in response to intense lobbying from the direct marketing industry, the text has been modified. It is no longer clear that Article 11 information has to be given before collection. This change should not prejudice the proper view that adequate information must be provided before collection. In the case of direct marketing, the point in issue is that individuals should be told that information about them is to be used not only for the specific transaction taking place but also to add their names to lists to be made available to other organisations. If individuals are not told before information is collected, they have no opportunity to reconsider the initial transaction. Giving a subsequent opportunity to 'opt out' tips the balance of inertia in favour of the data user who is compiling the marketing list. It hardly seems adequate to collect information unfairly and then provide the explanation as Article 11 currently seems to suggest. Indeed, that would seem to be a reduction in the protection given to individuals by the current UK Law.

5.8.5 Article 11 might well require modification to its drafting to introduce some flexibility as paragraph 5.8.3 suggests, but the Article should make it clear that as much of the explanation is to be given before collection as is practicable and the remainder as soon as practicable thereafter. In any case, the impracticality of giving an explanation in advance should not be used as a justification for acting unfairly to individuals; there should remain an over-riding duty to collect fairly.

5.9 Codes of Conduct (Articles 28 and 29)

5.9.1 There may be some doubt about how practical a Community-wide sectoral code of practice will prove to be. Nevertheless, codes of practice or conduct both national and at a community level could prove useful. The main concern is that these codes should neither be, nor be thought to be, some form of self-regulation allowing groups of data users to establish rules in conflict with, or in place of, the general requirements of the directive.

5.9.2 It is now clearer from the revised text that these codes are to be subordinate to the general legal duties, rather than in any way replacing them.

5.10 Automated Individual Decisions (Article 16)

5.10.1 The version of this Article in the original draft was drawn closely from the French Data Protection Law. It is based on a view that purely automated decisions are in some way more threatening to or invasive of personal privacy. The revised draft has been narrowed in two respects: first it is confined to decisions, "based solely on automatic processing defining a personality profile" and, secondly, exemptions have been included which

permit Member States a considerable discretion and, in particular, are designed to exclude credit scoring systems.

5.10.2 There may well be cases where the consistency of an automatic system is fairer to individuals than a personal judgment. The matter of importance is that the rules embodied in the system should be fair and justifiable and that the user of the system should be able to provide that justification when challenged. Article 13(5) goes some way in that direction but is not powerful enough. A remodelling of the two provisions would be welcome.

5.11 Compensation Rights

5.11.1 A distinctive benefit in both the original and revised drafts for individuals is in the right to compensation. Under the Act, individuals have rather limited rights to compensation in certain cases of inaccuracy, loss or destruction of data. The proposed directive would extend those rights to compensation to someone, "who suffers damage as a result of an unlawful processing or any Act incompatible with the national provisions adopted pursuant to the Directive". This extension is welcome but individuals should not thereby be deprived of their existing right to compensation in some cases for distress as well as damage.

5.12 Implementation Machinery

5.12.1 The revised draft requires Member States to establish supervisory authorities. There would be some enhancement to the current powers of the Registrar. These will be welcome especially where they would permit the Registrar to obtain further information in order to exercise his functions and especially where they would allow information to be obtained about the use of subject access exemptions.

5.12.2 The power under S.36(1)(3) of the Act to disseminate information is fundamental to the Registrar's role. Data Protection will be most effective when it has become part of the natural thinking of those collecting information and designing systems to ask themselves whether they have a need for the information, whether it is sufficient and accurate and indeed whether they have satisfied the other data protection principles. This long-term change in attitudes is a major educational task. The functions of supervisory authorities in Article 30 of the revised draft do not expressly include this educative function. It would be a retrograde step if the Registrar were deprived of such powers.

5.12.3 In Article 4, the proposal seeks to divide jurisdiction between Member States. The revised text no longer attaches jurisdiction to the physical location of the data but grants it to Member States in which controllers of data are established. It seems that this could still lead to multiple jurisdiction with unforeseen consequences. The policy and drafting of this Article need a careful review.

5.12.4 The revised draft establishes two Committees – one of Data Protection supervisory authorities and the other consisting of representatives of the Member States. The special role of the Member States' Committee is to assist the Commission in the exercise of the rule-making power given it in Article 33. The EC Data Protection Commissioners already meet frequently on an informal basis and there is merit in formalising that arrangement. It is not so clear that a subordinate rule-making power should be given to the Commission in such a sensitive policy area. If Article 33 were struck down, the need for the Committee representing Member States should be reviewed.

6. CONCLUSION

6.1 The Council of Europe Convention on Data Protection and associated national pieces of legislation arose from concern in the sixties and seventies

about human rights and the burgeoning power of computers and communications. The Convention relates to the privacy of individuals. It seeks to offer individuals some protection in circumstances where information about them is used by others.

6.2 There can be no such thing as absolute individual privacy. Balances need to be struck between the right to privacy and other public objectives. The Convention recognises this.

6.3 The Data Protection Act introduced measures of protection for individuals which have enabled the United Kingdom to ratify the Convention. However, unlike the Convention, the Act does not refer to privacy, it is simply a statute "to regulate the use of automatically processed information relating to individuals...". On the other hand, the European Community Draft Directive on Data Protection is concerned with privacy and, in its revised form, gives greater control and greater protection to individuals than the Act. It also, helpfully, reduces a bureaucratic burden on data users by allowing simpler registration procedures.

6.4 The revised draft is not perfect and there is still room for significant debate, for example, on the cover to be given to manual records and the position of the media. There are also other matters of substance or detail which need to be clarified. Nevertheless, the revised draft is welcome and not generally unreasonable in the broad balance it seeks to set at this stage between individual privacy and other public interests.

22 October 1992

Appendix 2

European Community (EC) Data Commissioners Conclusions on the EC Draft Directive on Data Protection Adopted at the Dublin, Boppard and Paris Conferences

A. Introduction

At their conferences in Dublin (14-15 December 1992) and Boppard (11-12 March 1993) the Data Protection Commissioners of Belgium, Denmark, France, Germany, Ireland, Luxembourg, the Netherlands and the United Kingdom have carefully examined the amended proposal for a Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data (COM (92) 422 final – SYN 287; Official Journal No. C 311/30, 27.11.1992). They have noted with satisfaction that the common conclusions adopted at their conference in the Hague (28-29 November 1991) and their subsequent submissions on notification have been taken into account to a very large extent.

At their conference in Paris (28-29 April 1993) the EC Data Protection Commissioners finalised their examination and discussion of the amended proposal, and adopted the present document with common conclusions for submission to the EC Commission, the EC Council Working Party currently studying the amended proposal, and the EC Parliament.

B. General Observations

The EC Data Protection Commissioners wish to see that the general purpose of the amended proposal is accomplished, which is to ensure that the protection of the rights and freedoms of individuals, notably the right to privacy, with regard to the processing of personal data is equivalent in all EC Member States, and in conformity with the principles and safeguards laid down in the Council of Europe Convention of 28 January 1981.

In this context they also agree with the observation in recital 9 that the approximation of national laws must not result in any lessening of the protection they afford but must, on the contrary, seek to ensure a high level of protection in the Community. This is particularly relevant for those countries which have considerable experience with national laws providing such protection at the moment.

Against this background the EC Data Protection Commissioners want to express some concern that the particular method of harmonisation, adopted in the amended proposal, may present problems in practice that need to be examined more closely.

While aiming at a high and equivalent level of protection in the Community, the proposal provides for general principles which need interpretation and specific application. This leaves a margin of appreciation for each of the Member States, which may have the effect that in some States there will be a stricter interpretation and application than in other States. Moreover, States may under certain conditions

derogate from certain provisions of the Directive. The result of all this is, that there may be different levels of protection in each of the Member States.

The EC Data Protection Commissioners appreciate the particular difficulties presented by a harmonisation of national laws in this area. They also support most of the arguments against a possible harmonisation in greater detail. Certain differences might therefore have to be accepted at the present time and subject to further harmonisation measures.

Under these circumstances it is essential that the limits set by the Directive are sufficiently clear and that the level of protection offered by the Directive is sufficiently high, so that unnecessary discrepancies can be avoided and existing legislation affording a high level of protection will not be prejudiced.

Where it is established that the existing law provides a higher level of protection than the proposed Directive the latter should be amended to meet this higher level of protection. In this spirit the following conclusions aim to draw attention to a number of points where the amended proposal could be further improved.

C. Detailed Comments

Article 1 – Object of the Directive

1. This Article only applies within the scope of the Directive as defined by Article 3. In other areas the Member States are not limited in their data protection policy. If there would be any doubt in this respect, the text should be clarified accordingly.

   It is also assumed that the provision of paragraph 2 does not preclude restrictions which result from a non-discriminatory application of national legislation in accordance with the Directive. Member States would have to be free to apply their own national law irrespective of whether a particular data flow takes place within its territory or across the borders (Cf. Explanatory report on the Council of Europe Convention, paragraph 67). If necessary, the text should be amended accordingly.

Article 2 – Definitions

2. The definition of "personal data" in Article 2(a) deals with the identifiability of a person. The first paragraph correctly stresses that persons can be identified in various ways, some of which are indicated here. However, the second paragraph should apply to all data – kept in detailed or in aggregated form – which is of such a type that the persons concerned can no longer be identified by reasonable measures.

   The EC Data Protection Commissioners assume that the Directive does not apply to deceased persons. If there is any doubt the point should be made explicit; it should be clear that it is for Member States to set out in the domestic legislation, where appropriate, the protection measures applicable to data relating to deceased persons.

3. The elements of the definition of "controller" in Article 2(d) should be limited to the issue of the purpose and the objective of the processing, with the consequence that the other elements mentioned (which data, which operations, which third parties) are to be considered as falling under the decision-making power of the controller thus defined. This will help to avoid practical problems where different parties are involved in the processing.

4. In Article 2(e) and elsewhere in the Directive the French equivalent of "processor" should be: sous-traitant.

5. The definition of "third party" in Article 2(f) is satisfactory, on the assumption that different legal entities belonging to the same conglomerate and different authorities would all be considered as third parties.

6. However, the use of the term "third party" is not always consistent. It seems to cover certain recipients, authorised third parties (legal authorities etc) and unauthorised third parties. In addition, the Directive makes reference to "recipients", a notion which is not defined. The meaning and the use of these terms need further clarification.

Article 3 – Scope

7. It should be clarified that the Directive applies to the processing of personal data, not only as long as they are the object of automatic processing or part of a manual file, but that they remain protected when taken out of this context and are used or disclosed by the controller, as is the case when data are communicated orally from a computer printout.

Article 4 – National law applicable

8. The provisions of this Article are unsatisfactory. If the law of the controller, as indicated in paragraph 1(a), would apply in all circumstances, only the supervisory authority established under that law would be competent, but it would lack the means to supervise activities taking place in other countries. It must be pointed out that the supervisory authority of the country hosting the activity would not be in a position to effectively supervise activities taking place in that country or elsewhere, and mutual cooperation between national authorities as mentioned in Article 30 would not make it possible to overcome this difficulty. A minimum condition for effective control would be that each national authority is competent to supervise the processing of personal data taking place within its jurisdiction. Therefore, at least to that extent the law of processing should apply.

However, other problems seem to be relevant too. On the basis of the present text there will be a need to apply the laws of other Member States in many cases. This might lead to great practical difficulties, especially in a legal system relying on criminal enforcement.

It is also doubted whether the law of the controller is always most suitable to apply to the collection of data from data subjects in other countries and to the use of their rights of access.

More in general, it should be kept in mind that differences in substantive law and notification systems – which are bound to arise or remain at this stage (cf. part B) – may lead to forum shopping.

In view of this, it is felt that the subject requires further study. In particular, it should be considered whether the establishment of the controller should not be combined with or replaced by other criteria, notably the place of the relevant activities.

Article 6 – Principles on data quality

9. The amended proposal does not establish the finality principle with sufficient clarity. In Article 6, paragraph 1(b), the principle is set out in a similar way as in Article 5(b) of the Council of Europe Convention. However, unlike that Convention the proposal does not determine whether and to what extent derogations from this provision could be allowed.

It is important that the Directive states clearly that such derogations under national or Community legislation are only acceptable if they are clearly

defined and limited in accordance with Article 9(2) of the Council of Europe Convention.

10. In view of the terminology employed in the Directive, the term "used" in Article 6, paragraph 1(b), should be replaced by "further processed".

Article 7 – Principles on grounds for processing

11. The provisions of this Article have been examined in the light of the conclusions adopted earlier at the conference in the Hague.

Although the general approach is very similar, the amended proposal fails to distinguish between lawful processing and lawful communication of personal data. It is suggested that Article 7 should be re-worded as follows:

Processing should be lawful only where:

— the data subject has consented (cf.Art.7,a);

— the processing is necessary for the performance of a contract (cf.Art.7,b);

— the processing is necessary for the fulfilment of a legal obligation (cf.Art.7,c);

— the processing is necessary for the execution of a public function or duty, provided that the finality principle be observed (cf.Art.7,e);

— the processing is necessary to safeguard the legitimate interests of the controller, on condition that the interests of the data subjects do not prevail (cf.Art 7,f, partim).

Communication of personal data to third parties should be lawful only on the grounds mentioned before (for processing in general), and where:

— the communication is necessary to safeguard the general interest or the legitimate interests of a third party, on condition that the interests of the data subject do not prevail (cf.Art. 7,f, partim);

— the communication is necessary in order to protect the vital interests of the data subject (cf. Art. 7,d).

At the same time concern has been expressed that the term "general interest" might be too wide and would include private business interests. This point needs further study in order to avoid any misinterpretation of the meaning of the words used in the different language versions.

Article 8 – Sensitive data

12. Paragraph 2(c) of this Article is a very general and vague exemption, and should therefore be deleted.

At the same time, paragraph 3 should not require specifications regarding the recipients and the controllers of data, nor should public interests be a prerequisite. It should be left to the Member States to strike the right balance between competing – private or public – interests and to provide the appropriate safeguards required in Article 6 of the Council of Europe Convention, within the general framework provided in the preceding Articles of the Directive.

13. The protection of this Article should apply to all criminal data, not only to criminal convictions. The exemptions which are available under paragraph 3 (amended), should also apply to these data.

Article 9 – Freedom of expression

14. In order to ensure that the freedom of expression is carefully balanced against the right to privacy, the beginning of this Article should read:

> "In so far as is strictly necessary in order to safeguard the freedom of expression, Member States shall...."

Article 11 – Collection of data

15. The beginning of this Article should provide that the information required should be given before or at the time of collection

16. The EC Data Protection Commissioners assume that the information under Article 11.1(d) (information on the destination of data) would place the data subject in a position to know of the existence of transborder flows of data.

17. The exception provided by paragraph 2 is too flexible. It should be available only when it is likely that an essential public function will be substantially hindered, and where the conditions described in Article 9.2a of the Council of Europe Convention 108 are satisfied.

18. Article 11 only applies where data are collected from the data subject, and not from other sources. To ensure that the transparency principle is respected more fully, it is felt that the data subject should be informed whenever he cannot reasonably expect that data have been stored about him, and where such information at the time of first disclosure of such data to a third party, as provided in Article 12, would be too late for an effective exercise of the data subject's rights, as eg in the case of credit information services. In this context, necessary and appropriate provisions should be introduced in order to avoid undue bureaucracy.

Article 12 – Disclosure to a third party

19. Paragraph 3 of this Article should be limited to cases where the supervisory authority establishes that to inform the data subject would be impossible or would involve disproportionate effort. In view of the exemptions provided in paragraph 2, the reference to overriding legitimate interests of the controller or a third party could be deleted.

Article 13 – Right of access

20. It is felt that the general idea underlying paragraph 2 could be expressed more effectively by a prohibition on any third party to ask a data subject to exercise his right of access, unless the request is founded on a proper legal basis.

Article 14 – Exceptions to the right of access

21. Paragraph 1 is too flexible. Member States should be entitled to provide for restrictions of the data subject's right of access only insofar as this is a necessary measure in a democratic society; and for the purposes mentioned in article 9.2 of Council of Europe Convention 108. Therefore this provision should be reconsidered.

22. The case in which Member States may limit the right of access to data to be processed for statistical purposes should be more strictly defined.

> We propose that this possibility should be restricted only to cases where the data are "temporarily kept in personal form and which is intended to serve exclusively statistical ends of such a type that the persons concerned can no longer be reasonably identified and where there is clearly no risk to the privacy of the data subject".

In addition, we propose that paragraphs 2 and 3 should be inverted so as to empower the control authority to carry out all the necessary checks, on its own initiative or at the request of the person concerned, to verify the lawfulness of the processing within the meaning of this Directive, respecting the interests to be protected in accordance with paragraph 1 and to ensure respect of the conditions laid down in paragraph 2 (former paragraph 3 concerning statistics).

Article 15 – Objection on legitimate grounds

23. The words "by mail" at the end of paragraph 3 should be deleted.

Article 17 – Security

24. In paragraph 1 the word "use" should be inserted after "and against unauthorised".

Article 18 – Notification

25. For practical purposes, the place where to exercise the right of access should be added to paragraph 2(a) where this differs from the address of the controller.

26. In paragraph 4, the words, "within a period of 15 days commencing with the date of the notification" should be replaced by the words "within a reasonable time".

Article 19 – Simplification and exemption

27. The EC Data Protection Commissioners request the deletion of the second sentence of Article 19.1 which lists by way of indication the categories of processing which may be subject to simplification and exemption and does no more than illustrate the principle set out in the first sentence, which is sufficient in itself.

28. The first part of paragraph 2 should state that "the simplification or exemption measure is to be taken by legislative means or administrative means, in the latter case by the control authority or after consultation with it".

Article 30 – Supervisory authority

29. It is understood that each supervisory authority should have at least the powers mentioned in paragraph 2. However, other powers are not excluded.

The notion of "effective powers of intervention" as stipulated in this paragraph, should cover administrative decisions as well as the ombudsman type of intervention, including the power to report to Parliament and to the public. If needed, this should be clarified in the text.

As to the power of the supervisory authority to initiate judicial activities, mentioned in the same paragraph, substantial differences have appeared between the French, English and German versions. This power should not be limited to penal procedures. Moreover, in the French version the word "infractions" should be replaced by "violations".

In addition the EC Data Protection Commissioners are convinced that there is an important role for the supervisory authorities to play in providing information and advice on the protection of personal data.

Article 31 – Working Party

30. This Article has been improved on a number of points. In its present form, it can be considered as an essential element of a harmonised data protection policy.

Article 32 – Tasks of the Working Party

31. Paragraph 1 should be completed by a new sub-paragraph:

> "e) monitor new information processing methods and techniques."

Paragraph 5 of this Article should provide that the Commission shall inform the Working Party of Community research projects which imply the automatic processing of personal data.

32. A new paragraph 1 bis should be inserted as follows:

> "The Working Party shall be consulted by the Commission on any proposed decision referred to in Article 26(5), any codes referred to in Article 29, any measure proposed to be adopted by the Commission under Article 27(3), and any measure proposed to be taken under Article 33 of the Directive."

Article 36 – Final Provisions

33. In this article, it should be stated that the Commission also has to report on developments in national data protection laws.

D. Final Observation

The EC Data Protection Commissioners also encourage the Community to provide for regulations applicable to the services of the Community and to establish an independent data protection authority to control their compliance. Referring to their Berlin Statement of August 30, 1989, the Commissioners underline that the amount of personal data processed by the services of the Community Authorities is already considerable but will grow dramatically as a consequence of the Maastricht Treaty.

Appendix 3

The Office of the Data Protection Registrar
NHS Contract Minimum Data Sets

Report of an investigation to consider whether the collection, content and use of contract minimum data sets in the National Health Service could lead to contravention of the requirements of the Data Protection Act.

SUMMARY OF FINDINGS

Reforms in the National Health Service have included the introduction of a form of internal market. There are organisations that directly provide individual health care. These are known as "providers". Very often they are hospitals. There are separate organisations responsible for purchasing this health care for the population they serve. They pay the providers. These organisations are known as "purchasers". Contracts are in place between purchasers and providers. When a provider treats a patient, a standard set of information about the patient is sent to the purchaser. This set of information is known as the contract minimum data set.

A complaint was received by the Registrar about the content and use of contract minimum data sets. The complaint addressed the Fourth Data Protection Principle which requires that personal data are adequate, relevant and not excessive and the Eighth Data Protection Principle which requires that personal data are kept secure. In investigating the complaint the Registrar also considered the implications of contract minimum data sets for compliance with the First Data Protection Principle which requires that personal data are obtained and processed fairly and lawfully, and the Sixth Data Protection Principle which requires that personal data are kept for no longer than is necessary.

Responsibility for compliance with the Data Protection Principles in the National Health Service falls on individual purchasers and providers. The Department of Health has a role in enabling and encouraging purchasers and providers to meet their responsibilities but its direct responsibilities extend only to personal data held by the Department itself. Whilst the overall content of contract minimum data sets is laid down by the Department of Health each purchaser and provider must be able to justify the holding of items of personal data by the use it makes or intends to make of them. It is not sufficient justification for a purchaser or provider to collect and hold data items for no other reason than that they form part of a contract minimum data set.

Contract minimum data sets are held for several different purposes by hundreds of different purchasers and providers and may relate to millions of different individuals. Given the range of practices adopted by these purchasers and providers it is difficult to envisage that complete compliance with the Data Protection Principles can be achieved if the full contract minimum data set is collected and held on every patient in every case.

The aim of this investigation was to consider whether the collection, content and use of contract minimum data sets in the National Health Service could lead to contravention of the requirements of the Data Protection Act. It has revealed that for the most part providers and more particularly purchasers have not reviewed their

own practices in connection with contract minimum data sets to ensure compliance with the Data Protection Principles. They are generally relying on the assumption that because they are holding a standard data set, the content of which is laid down centrally by the Department of Health rather than determined locally, they will not breach the Principles. Such an approach will in many cases lead to contraventions of the requirements of the Data Protection Act.

Areas of particular concern include the holding of patient identifiers other than the NHS number, the holding of data on a patient's marital status and more generally the holding of personal data for research with no clear plans as to how the information will be used.

The principal conclusions of the investigation on measures needed to promote compliance with the Act's requirements are:

(i) Providers should review their data collection practices to ensure that they obtain information fairly from patients making certain that patients are aware of the uses and disclosures of their information that are associated with contract minimum data sets.

(ii) A guidance note on the application of the "fair obtaining" requirements of the First Data Protection Principle in the NHS should be published by the Registrar.

(iii) Purchasers and providers should individually review the extent to which they hold items of personal data from contract minimum data sets to ensure that the data they hold are adequate, relevant and not excessive for each of their purposes. Particular attention should be given by purchasers to the holding of personal identifiers, the holding of data on marital status and the need to have clear plans as to how any data items held for Research and Statistical Analysis and/or Public Health will be used.

(iv) Purchasers, whilst ensuring they meet any statutory requirements for the retention of information, should adopt a systematic policy for the deletion of personal data from contract minimum data sets to ensure that information is not held for any longer than is necessary.

(v) Purchasers and providers should, in the light of the NHS Management Executive's Code of Practice for the Handling of Confidential Patient Information in the Contracting Environment, individually review, develop and implement procedures that will ensure the security of sensitive personal health information held in contract minimum data sets.

(vi) A Data Protection Code of Practice for purchasers in the NHS should be developed by a suitable representative body with the encouragement and assistance of the Registrar.

(vii) The Department of Health through its NHS Management Executive should be approached by the Registrar to continue or, where necessary, initiate discussions and action on the issues raised by the investigation. Particular attention will be drawn to:

  (a) the need for purchasers and providers to review their data handling practices to ensure compliance with the Data Protection Principles;

  (b) the extent to which purchasers need to hold patient identifiers and the length of time for which they are held;

  (c) the need for purchasers holding contract minimum data sets for Research and Statistical Analysis and/or Public Health to have clear plans as to how

they will use the personal data they hold;

(d) the continued inclusion of "marital status" as a data item in contract minimum data sets;

(e) the proposed inclusion of "ethnic origin" as a data item in contract minimum data sets;

(f) the identification of a suitable representative body to develop a Data Protection Code of Practice for purchasers;

(g) the application of the "fair obtaining" requirements of the First Data Protection Principle to providers;

(h) the reissue and increased use of the NHS number.

February 1993

Appendix 4

Guidance Note 27

Views of the Data Protection Registrar Concerning Revised Enforcement Notices Issued Against Four Credit Reference Agencies By The Data Protection Tribunal

INTRODUCTION

1. This Guidance Note deals with the meaning and effect of the Enforcement Notices issued by the Data Protection Tribunal to the four main credit reference agencies in the U.K. which come into effect on 31 July 1993. In preparing this guidance, the Registrar has taken account of views on an initial discussion paper sent to each of the four agencies, inviting comments from them on the points raised in it.

2. This guidance has been produced following the Registrar's consideration of the Notices and highlights those areas of the Notices which, in his view, will benefit from detailed consideration at this stage. The guidance is not intended to be a line by line analysis of the Notices. It does not cover all circumstances, and any complaints received by the Data Protection Registrar that lead him to believe that an Enforcement Notice may have been breached will be considered on the facts of each case.

3. One effect of the Notices may be to raise questions about other areas, for example the notifications given to individuals who make credit applications. These questions are not addressed in this Guidance Note.

4. The Registrar recognises that the agencies are working under considerable time pressures in order to produce new systems. He hopes his contribution will enable agencies to take account of his views in the production of those systems.

STRUCTURE OF THE GUIDANCE NOTE

5 Issues and questions arising have been grouped under a number of main headings:

a. Electoral Roll Information.

b. Residence.

c. Name Matching.

d. "Family" Membership.

e. Disassociation.

6. To some extent these divisions are artificial; for example there are also comments on the use of the electoral roll under residence and "family" membership. References to paragraph numbers are references to the paragraphs in the Enforcement Notices. A copy of the wording of the Enforcement Notices is at the end of this Guidance Note for ease of reference. The Enforcement Notices appeared at paragraph 3 of each of the Tribunal's Appeal Decisions. The numbering of references in this Guidance Note reflects this.

ELECTORAL ROLL INFORMATION

7. Paragraph 3(1) refers to *"personal data relating to the financial status of*

individuals" and to "*any financial information*". The first phrase comes from the Data Protection Registrar's standard purpose for Credit Reference. Prima facie, electoral roll information falls outside the terms of the Notice. This view is based on the understanding that the current use of electoral roll information about third parties is limited to ascertaining the presence of persons other than the applicant for credit at an address and that this information is not credit scored or otherwise used to assess the applicant for credit. If the practices current at the time the Tribunal settled the Notice were to change, the Registrar would consider any complaints made to him in the light of the terms of the Notice, and if necessary he would consider further enforcement action. Credit Scoring and the geodemographic association of data, for example for direct marketing purposes, are outside the scope of the Enforcement Notices and can be discussed separately with the Registrar's staff.

RESIDENCE

8. Paragraph 3 (2) refers to: "*information about any other individual recorded as residing at the same present address or previous address as the subject*". The initial test of the sequence of tests in the proviso in paragraph 3(2) requires that the third party and the applicant for credit are recorded as residing at the same address. The Registrar's view is that as a matter of fact the "same address" is the same residential unit.

9. In respect of previous address it should be noted that the proviso only permits the extraction of *third party* information from a maximum of *two* addresses: the current address and the previous address.

10. The Registrar's view is that an individual is *recorded as residing* at an address if he is on the electoral register at that address; in the absence of further information to contradict it, an agency would expect to be able to rely on this insofar as it will confirm that the individual was resident at the address on 10 October prior to the publication date of a specific electoral register.

11. As Credit Reference Agencies normally hold records supplied to them by others, they must assess carefully whether other categories of information show that an individual is *recorded as residing* at a particular address. Information obtained from third parties that does not purport to show that an individual is *recorded as residing* at a particular address should not be assumed to do so, (eg the Royal Mail Postal Address File).

12. Not every agency holds the same information. However County Court Judgment (CCJ) information is held by all the agencies. The provisions of the County Court Rules allow any address to be given for service; there is no requirement in the Rules that the individual be *resident* at that address and the information does not come directly from the individual him/herself. In these circumstances there is some risk if an agency relies on CCJs alone as showing that an individual is *recorded as residing* at a particular address unless an agency holds additional information to support that assertion.

NAME MATCHING

13. The issues raised here concern paragraphs 3(2)(a)(i); 3(2)(a)(ii); and 3(2)(b)(ii). They can be divided into two separate matching exercises, the first, 3(2)(a)(i) being whether the forename or initials, where these are recorded, are the same. This is an absolute test of fact with no element of belief. The second, 3(2)(a)(ii) and 3(2)(b)(ii), concerns the matching of *sufficiently similar* names. This imports a test of *reasonable to believe* into the final assessment of whether the names match sufficiently to be viewed as either the same person or as a third party having the same surname. It is the Registrar's view that *reasonable* as used in the Notice embodies an objective test.

14. The test contemplated by paragraphs 3(2)(a)(ii) and 3(2)(b)(ii) is an objective

test. It is for the agency to satisfy the objective test. The Registrar considers that an agency should take extreme care in reaching its judgment as to whether two names may be sufficiently similar to be believed to be the same. It is the Registrar's view that a double-barrelled surname such as SMITH-BROWN may not be sufficiently similar to either the surname SMITH or BROWN, to be extracted, no more may WILLIAMSON be sufficiently similar to WILLIAMS. However, the Registrar considers that it is difficult to frame comprehensive examples as each case must be judged on its facts as to whether or not it satisfies the objective test. In any given case the answer may depend on other information held.

15. Where inherent contradictions are apparent in the data held, (an example of this would be where there is a difference in sex implied by the title) it is clear there can be no extraction when assessing similarity of name. In the absence of inherent contradictions and where the provisos of paragraphs 3(2)(a)(i), 3(2)(a)(ii) and 3(2)(b)(ii) are met, data may be extracted.

FAMILY MEMBERSHIP

16. In relation to the phrase used in 3(2)(b) – and the similar phrase used in 3(2)(c) – *and where in either case it is reasonable to believe that he or she has been living as a member of the same family as the subject in a single household*, it should be noted that in order to meet this requirement the third party must, firstly, have been living as a member of the same family as the subject and, secondly this must have been in the context of the family being a single household. It is the Registrar's view that both parts of the condition must be satisfied before it can be said to apply to the third party.

17. This has to be considered in relation to the addition to the similar requirement in 3(2)(c) that the belief be based upon *information obtained before extraction*. The Registrar would not accept any assumption that two persons with different surnames shown on the electoral roll at the same time at an address, had any particular relationship. In the absence of other information, if the same or sufficiently similar surnames are recorded as residing concurrently at the same address, the Registrar accepts that this may be the basis for a reasonable belief that they are living as members of the same family in a single household providing no party has disassociated him/herself from the group. The Enforcement Notices do however envisage that two people may live together as members of the same family in a single household without there being a financial connection between them.

DISASSOCIATION

18. There is no requirement in the Notice that an individual will have to file a Notice of Correction or otherwise comply with any particular formalities in order to make a disassociation. If an agency wishes to rely on the proviso to the Notice in order to extract third party information then the agency must accept all the terms of the proviso including the disassociation provision in 3(3). This provision refers to *information in the possession of [the agency]*. It does not distinguish in which capacity the information is held or whether it is subject to any other contractual provision. It therefore appears to bite on all information in the possession of the agency in whatever capacity it is held. In the Registrar's view this would cover subscriber information and closed user group information held by the agency. It would not be open to an agency to ignore such information in its possession when assessing third party information even where the agency's customer for whom the search is carried out is not a subscriber or member of the group.

19. It is possible for an agency to comply with the Notice and lawfully extract by limiting its extraction solely to information about the applicant for credit. If an agency is not prepared to apply closed user group information to searches

conducted on behalf of its customers who are not members, then the agency can limit its searches to information about the applicant for credit.

20. Any disassociation must have a two-way effect in relation to data that would otherwise be extracted as part of the same file or search request. Thus if Mary Smith successfully disassociated herself from John Smith, data about John Smith would not be available on a search relating to Mary Smith and vice versa.

21. It is accepted that Credit Reference Agencies will not always be able to accept at face value claims of disassociation by every individual. Where there are reasons not to do so, enquiries may need to be made to ascertain the facts of a case. This may result in delay in recording a disassociation. To ameliorate this problem an agency, once a disassociation has been recorded, should inform those who have made enquiries about an individual during the period between receipt of the disassociation by the agency and its addition to the record.

ADDITIONAL COMMENTS

22. Agencies should be mindful of how they would proceed in the event of a query about whether the extraction of third party information had come within the terms of the proviso or not. Bearing in mind that an agency might have to prove a proper use of the proviso in a court of law it might be appropriate for agencies to consider whether new systems should not only determine whether extraction should take place but identify and record which section(s) of the proviso are being relied upon.

FEBRUARY 1993

Annex to Guidance Note 27

Text of the Revised Enforcement Notices

3. (1) That, subject to paragraph (2) below, from 31 July 1993 (name of credit reference agency) shall cease to extract **personal data relating to the financial status of individuals** by any extraction program whereby (i) such personal data is extracted by reference to the current or previous address or addresses of the subject of the search ("the subject") and (ii) there is extracted, in addition to information about the subject, any **financial information** about any other individual who has been recorded as residing at any time at the same or similar, current or previous, address or addresses as the subject.

(2) Subject to paragraph (3) below, nothing in this notice shall prevent the extraction of **information about any other individual, recorded as residing at the same present or previous address as the subject** concurrently with the subject, who -

(a) (i) has the same surname, and forenames or initials **where these are recorded,** as the subject, or

(ii) has a name sufficiently similar to that of the subject for it to be reasonable to believe that he or she is the subject, or

(b) (i) has the same surname as the subject, or

(ii) has a surname sufficiently similar to that of the subject for it to be reasonable to believe that it is the same surname,

and where in either case it is reasonable to believe that he or she has been living as a member of the same family as the subject in a single household, or

(c) does not have the same surname as the subject but in respect of whom, on the basis of information obtained before extraction, it is reasonable to believe

(i) is the subject or

(ii) has been living as a member of the same family as the subject in a single household.

(3) In Paragraph (2) above -

sub-paragraphs (a) and (c) (i) shall not apply where there is information in the possession of (name of credit reference agency) from which it is reasonable to believe that the individual is not the subject;

sub-paragraphs (b) and (c) (ii) shall not apply where there is information in the possession of (name of credit reference agency) from which it is reasonable to believe that there is no financial connection between the individual and the subject.

Appendix 5

Awareness Activities – Statistics From 1985

The statistics are shown on a year by year basis. The reporting year is from 1 June in one year to 31 May in the next.

(a) USE OF THE ENQUIRY SERVICE

	Telephone Enquiries	Letter Enquiries
1985	5,000	5,000
1986	80,000	23,000
1987	17,000	6,000
1988	42,000	10,000
1989	32,000	7,500
1990	41,000	8,500
1991	41,000	7,500
1992	39,000	13,000
1993	43,000	16,000
TOTAL	340,500	96,500

(b) PUBLIC RELATIONS

	Press Conferences	Press Releases	Press Mentions	Radio & TV Interviews	Talks at Seminars & Conferences	Radio Tapes for Free Transmission
1985	n/a	5	n/a	10	50	–
1986	1	16	2,003	45	150	1
1987	1	14	1,137	19	37	1
1988	2	23	1,663	93	73	–
1989	1	13	933	24	51	2
1990	1	22	1,500	33	43	–
1991	1	27	1,400	22	56	–
1992	1	24	1,500	23	53	–
1993	2	19	1,000	14	100	–
TOTAL	10	163	11,136	283	613	4

(c) NUMBER OF PUBLICATIONS DISTRIBUTED

	First Published	Approximate Total Number Distributed to Date
Guideline No 1 (Blue)	February 1985	Over 500,000
Questions and Answers 1-20	September 1985	150,000
Questions and Answers 21-34	February 1986	150,000
Update No 1	November 1985	230,000
Update No 2	July 1987	200,000
Update No 3	October 1988	200,000

	First Published	Approximate Total Number Distributed to Date
Update No 4	March 1991	160,000
Update No 5	March 1992	180,000
Update No 6	December 1992	143,000
Guideline No 1 (Red)	March 1987	150,000
Guideline No 2	March 1987	85,000
Guideline No 3	March 1987	85,000
Guideline No 4	March 1987	88,000
Guideline No 5	March 1987	88,000
Guideline No 6	March 1987	90,000
Guideline No 7	March 1987	85,000
Guideline No 8	March 1987	85,000
Guideline No 1 (Revised)	February 1989	98,500
Guideline No 2	February 1989	34,500
Guideline No 3	February 1989	33,500
Guideline No 4	February 1989	40,500
Guideline No 5	February 1989	47,000
Guideline No 6	February 1989	47,500
Guideline No 7	February 1989	32,000
Guideline No 8	February 1989	32,000
Guideline Sets 1-8	February 1989	270,000
Guidance Notes	From 1985 onwards	25,500
"Insights"	June 1991	9,500
"What is Data Protection" (Intro leaflet)	Sept 1991	112,000
Are you in on the Act? (Rights Leaflet)	Nov 1987	1,993,000 *(inc. 1,000,000 inserts in Women's magazines)*
Professional Advisers Pack	Feb 1986	27,250
"Important Message" card for new data users	Oct/Nov 1988	68,000
"Resource Pack" for schools	1987 and 1988	7,500
Professional Advisers Pack	Feb 1992	3,500
Video	July 1992	3,000

(d) NEWSPAPER ADVERTISING

Campaign	Date	Media
Data User (Registration)	Nov/Dec 1985	National Dailies/Sundays and Regional
Data User (Registration)	Mar/Apr 1986	National Dailies/Sundays and Regional
Professional Advisers (Solicitors and Accountants)	Sept 1987	Small Business and Professional Journals
Data Subject (Full rights available)	Nov/Dec 1987	National Dailies/Sundays and Regional
Data Subject	Mar 1988	National Dailies/Sundays and Regional
Data Subject	July/Aug 1988	National Dailies/Sundays and Regional
Data Subject	Oct/Nov 1988	National Dailies/Sundays and Regional
Data Users (fee increase)	Nov/Dec 1988	Trade Press
Data Users (fair obtaining)	Feb/Mar 1989	Trade Press

Campaign	Date	Media
Data Subject (subject access)	Mar 1989	National Dailies
Data Users	Oct/Nov 1989	National Press
Data Users (fee increase)	May 1991	National Press
Professional Advisers	February 1992	Professional Journals and Trade Press

DIRECT MAIL ADVERTISING

Campaign	Date	Target
Professional Advisers (Adviser's Pack)	Feb 1986	Solicitors and Accountants (27,000)
Small Businesses (Simplified Registration Form)	Sept 1987	(250,000)
Professional Advisers (Simplified Registration Form)	Sept 1987	Solicitors and Accountants and Small Firms Advisers (33,000)
Professional Advisers (Fee Increase)	Oct 1988	Solicitors and Accountants and Small Firms Advisers (56,000)

TELEVISION ADVERTISING

Campaign	Date	Media
Data Subjects	Mar/Apr 1990	National Television
Data Subjects	Mar 1992	Channel 4 (Midlands, North West, Scotland), Satellite TV

Appendix 6

Research Results

In order to monitor attitudes and knowledge about data protection and related issues, amongst the public at large and amongst business establishments, research is undertaken from time to time. The work is carried out by professional research organisations under the direction of the Central Office of Information (COI). The COI analyses the results of the research and prepares tables and commentaries. Extracts from the tables and commentaries are reproduced in this Appendix. They fall into two classes – those results relating to members of the public and those relating to business establishments.

(a) *Members of the Public* (Tables 1 to 9)

The tables show the main results of the research undertaken over the last three years. However, research has taken place annually since 1987. The full research results for the current and past years are available for study by interested parties.

The research method was to conduct face to face interviews with a representative sample of the population selected by a mixture of random and quota methods. The sample size at each stage was around 1,000.

(b) *Business Establishments* (Tables 10 to 13)

The tables show the main results of the research undertaken in the last three years. However, research has taken place in the first half of the year since 1986. The full research results for the current and past years are available for study by interested parties.

The surveys were conducted by telephone. There were 2,000 interviews with a representative sample of business establishments with less than 50 employees and 400 interviews with a representative sample of business establishments with 50 employees or more. The sample of business establishments was drawn from British Telecom's business database.

(c) *Statistical Significance*

In the tables, ** denotes a difference between two percentages which is statistically significant at the 95% level. The probability of a marked difference arising simply from sampling variation is 1 in 20 or less.

In calculating significance a design factor of 1.2 has been applied in recognition of the clustered nature of the sample in which sampling error will have been greater than for a pure random sample of the population, in which each individual had an equal opportunity of being selected.

Table 1

Members of the public were asked to choose, from a list of issues, those which they considered to be very important.

	1991		1992		1993
	%		%		%
Proportion saying the following are very important:					
Preventing crime on the streets	83	**	91	**	85
Improving standards of education	78	**	82	**	78
Protecting peoples rights to personal privacy	73	**	78	**	66
Unemployment	70	**	80		78
Inflation	62		66	**	46
Protecting freedom of speech	58	**	67	**	53
Making sure women have equal rights	54	**	61		57
Protecting the rights of minority groups	35	**	40		40

** = statistically significant.

Comment:
1993 has shown a significant decline in respondents perceiving 'preventing crime on the streets', 'personal privacy,' 'inflation', and 'freedom of speech' as very important.

Table 2:

Members of the public were asked to name the five privacy issues which were of most concern to them. They were given a list of issues from which to choose.

	1991	1992	1993
	%	%	%
Proportion saying the following are of most concern:			
Keeping personal information/ details private	74	76	73
Protecting the privacy of your own home/property	74	78	79
Being able to do what I want in my own home	63	64	66
People telling me what to do/ interfering with my life	57	58	58
Organisations building up files of information about me	51	52	49
Maintaining freedom of movement/speech/ religion	51	50	53
Stopping unwanted mail/telephone calls/selling	56	51	49
Individuals prying into my business	52	52	53

Comment:
There has been no change in the privacy issues of most concern to people.

Table 3:

Members of the public were asked to say how concerned they were about the amount of information that is kept about them by various organisations.

	1991	1992		1993
	%	%		%
Very concerned	40	39	**	33
Quite concerned	32	34		35
Neither/Nor	8	8		11
Not very concerned	13	12		15
Not at all concerned	6	5		5

** = statistically significant

Comment:
1993 shows a fall in the number of people very concerned about the amount of personal information kept by organisations.

Table 4:

Members of the public were given a list of different types of information and asked to indicate their level of concern about organisations keeping this information without their knowledge.

	1991	1992		1993
	%	%		%
Proportion saying very or quite concerned:				
Your savings	74	77		75
How much you earn	67	72		70
Court judgements	64	67		67
Credit ratings	64	68		65
Your visitors	57	60		59
Medical history	61	61		62
Education and job history	44	43		40
What you buy	34	39	**	32
Membership of clubs	27	27	**	22
Your TV viewing	12	12		12
What papers you read	18	14		15
Your age	14	15		15

** = statistically significant

Comment:
There has been a significant decline in concern about information being kept on purchases and membership of clubs.

Table 5

Members of the public were asked to say how satisfied they were that various organisations can be trusted to keep and use information in a responsible way.

	1991		1992		1993
	%		%		%
Doctors and the NHS					
Satisfied	91		92		92
Not satisfied	5		5		3
Banks and building societies					
Satisfied	83	**	78		75
Not satisfied	10		13		16
Employers					
Satisfied	75		74		72
Not satisfied	10		11		11
Police					
Satisfied	69		72	**	78
Not satisfied	20	**	15		12
Inland Revenue					
Satisfied	66		68		68
Not satisfied	19		17		15
Schools and colleges					
Satisfied	65		66		70
Not satisfied	12		12		7
DHSS					
Satisfied	61		63		65
Not satisfied	18		16		15
Shops and stores					
Satisfied	35		36		32
Not satisfied	39		41		40
Credit reference agencies					
Satisfied	31	**	25		30
Not satisfied	44		49		41
Mail order companies					
Satisfied	23		23		23
Not satisfied	53		57		54

** = statistically significant:

Comment:
There has been an increase in the proportion 'satisfied that they can trust the police to be responsible with data'.

Table 6

Members of the public were asked to say what importance they attached to various rights.

	1991	1992	1993
	%	%	%
Proportion saying the following rights are very important:			
To correct errors in information about yourself	84	83	84
To know what the information about you is being used for	81	80	80
To be told who the information about you is being passed to	83	83	83
To be told where the information about you came from	78	77	80
To see what information is held about you	79	77	79
To have yourself removed from lists or files	75	78	75
To add things to the information about yourself	66	68	69

Comment:
These figures have remained very stable throughout the course of the research.

Table 7

Members of the public were asked questions to ascertain whether they were aware of the Data Protection Act, whether they had used the Act and how useful they considered the Act to be.

	1991	1992		1993
	%	%		%
Aware that there is a law concerning rights about information kept on individuals	22	22		20
Spontaneous awareness of the Data Protection Act	8	9		8
Prompted awareness of the Data Protection Act:				
Definitely heard of	18	20		20
Think so	11	9		12
TOTAL AWARENESS OF THE DATA PROTECTION ACT	37	38		38
Made use of the Data Protection Act	3	3		4
Think the Data Protection Act is very useful	66	67	**	61
AWARENESS OF THE DATA PROTECTION REGISTRAR	36	34		35
TOTAL AWARENESS OF DATA PROTECTION*	53	51		53

* = Anyone who has either definitely heard or thinks he or she has heard of the Data Protection Act and/or heard of the Data Protection Registrar.
** = statistically significant

Comment:
There has been no change, apart from a drop in the proportion who think that the Data Protection Act is very useful.

Table 8

Without prompting, members of the public were asked to say what they knew about the Data Protection Act.

	1991		1992	1993
Base: all aware of the Data Protection Act	370		384	381
	%		%	%
Right to find out what information is held about you	26	**	16	15
Protecting your rights about what information is kept on you	13	**	21	19
Firms need to register	7		6	7
Have to pay	2		1	2
Able to correct wrong information	11		7	3
Only see computer records	2		2	1

** = statistically significant

Comment:
No change from last year. The significant changes between 1991 and 1992 have been sustained.

Table 9

Members of the public were asked to indicate which functions they thought the Data Protection Act performed.

	1991		1992	1993
Base: all aware of the Data Protection Act	370		384	381
	%		%	%
Proportion saying the Data Protection Act performs the following functions:				
Enforcing your right to see information kept about you	64		63	62
Enforcing your right to correct information kept about you	65		62	61
Controlling information that can be kept on you	53		56	48
Monitoring all personal information on paper as well as on computer	33		35	40
Stopping organisations passing information about you to others	35	**	43	44
Making people who misuse information liable to imprisonment	35		40	35
Providing compensation if you are harmed by the misuse of information	24		29	28

** = statistically significant

Table 10

Businesses were asked about their use of computers.

	Small Companies (Fewer than 50 employees)			Large Companies (50+ employees)		
	1991	1992	1993	1991	1992	1993
Sample size:	2001	2047	2005	396	402	408
	%	%	%	%	%	%
Type of computer:						
Personal/micro	27 **	35	37	89	89	96
Multi-user or mini computer	9	10	10	71	73	66
Word processor	20	19	24	81	70	63
Computer access terminal	8	7	8	49	45	47
Mainframe	5	4	4	36	35	27
Data processing carried out by outside body	6	4	6	25	28	22
TOTAL with computers or use computer bureau	45 **	50	53	100	100	100

** = statistically significant

Table 11

Those businesses which used computers were asked whether they held personal records on them.

	Small Companies (Fewer than 50 employees)			Large Companies (50+ employees)		
	1991	1992	1993	1991	1992	1993
Base: all using computers	1036	1134	1144	393	402	408
	%	%	%	%	%	%
Hold personal records on computer						
Yes	43	46 **	51	97	100	100
No	52	50	47	–	–	–
Don't know	4	4	2	3	–	–

** = statistically significant

Comment:
There has been an increase in the proportion of small establishments that hold personal records on computer.

Table 12

Those businesses which hold personal records on computer were asked about their awareness of the Data Protection Act and the Data Protection Registrar.

	Small Companies (Fewer than 50 employees)			Large Companies (50+ employees)		
	1991	1992	1993	1991	1992	1993
Base: all who hold personal records	520	533	600	383	402	408
	%	%	%	%	%	%
Prompted awareness of the Data Protection Act	87	88	87	95	97	97
Semi-prompted awareness of the Data Protection Registrar*	47 **	58	54	61 **	72	75

* Respondents were asked to select from a list of likely sounding titles the person responsible for looking after the public's interest with regard to personal records held on computer.

** = statistically significant

Table 13

All businesses holding personal records on computer were asked questions to ascertain their awareness of the need to register under the Data Protection Act and that the Act imposes other obligations (for example compliance with the Data Protection Principles).

	Small Companies (Fewer than 50 employees)			Large Companies (50+ employees)		
	1991	1992	1993	1991	1992	1993
Base: all who hold personal records	520	533	600	383	402	408
	%	%	%	%	%	%
Aware of the need to register	62	62	59	82	85	85
Awareness of other obligations (as well as the need to register)	26	29	29	44	45 **	56

** = statistically significant

Comment:
Awareness of other data user obligations has risen amongst large companies. Awareness of the need to register is connected with size. Over the last three years awareness has been consistently lower in both the large and the small establishment samples among the smallest size categories (1-2 employees and 50-199 employees respectively). Awareness has also been consistently lower over the last three years among respondents from the distribution sector in both the large and the small establishment samples.

Appendix 7

Data Protection Registrar

Statement of Account for the Year Ended 31 March 1993

Data Protection Act 1984

FOREWORD

Background Information

1. The Registrar was appointed on 20 September 1984 under Section 3(2) of the Data Protection Act 1984. This Account has been prepared in accordance with Section 7(1)(b) of Schedule 2 to the Act. The Account covers the year 1 April 1992 to 31 March 1993.

Review of Activities

2. The purposes of the Act are to:

   - make the nature and use of personal data in computing systems open to public scrutiny (through a public register and by enabling individuals to obtain details of information about themselves);
   - ensure good practice in the use, processing and protection of personal data in computing 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 or from inaccuracies in such data.

3. Contributions continue to discussions on the European Community Draft Directive on Data Protection. The final directive is likely to set the stage for United Kingdom legislation for the late nineties.

A brief advertising campaign very substantially increased the flow of complaints from individuals about uses of information held about them. This seems to indicate that there is a latent concern to be addressed.

Enforcement actions in respect of the obtaining of information for direct marketing are awaiting a hearing before the Data Protection Tribunal. The application of the Act has led to improved practices in this area which have reduced relevant complaints.

A variety of other activities relate to such as policing, the health service and banking practice.

Events since the end of the Financial Year

The Ninth Annual Report of the Data Protection Registrar will be laid before Parliament on 13 July 1993. This gives fuller details of activities.

E.J. HOWE CBE
Data Protection Registrar

16 June 1993

STATEMENT OF RECEIPTS AND PAYMENTS ACCOUNT FOR THE YEAR ENDED 31 MARCH 1993

	Notes		*1992/93*		*1991/92*
		£	£	£	£
H.M. Grants received	2	3,744,169		3,423,094	
Operating receipts	3	7,726,669	11,470,838	2,254,965	5,678,059
Salaries and Wages		1,537,864		1,351,156	
Other operating payments	4	2,127,335	3,665,199	1,957,527	3,308,683
Surplus from operations			7,805,639		2,369,376
Other Receipts	5	115,377		169,749	
Other Payments	5	58,256	57,121	92,630	77,119
Surplus for Year			7,862,760		2,446,495
Appropriations	6		7,628,141		2,446,915
Excess of receipts over payments (payments over receipts) for the year			234,619		(420)

STATEMENT OF BALANCES AS AT 31 MARCH

	Note	*1993*	*1992*
		£	£
Balance at beginning of year		23,810	24,230
Excess of receipts over payments (payments over receipts) for the year		234,619	(420)
	7	258,429	23,810

The Notes on pages 106 and 107 form part of this account.

Notes to the Statement

		1992/93 £	1991/92 £
1.	This account is drawn up in a form directed by the Secretary of State, and approved by the Treasury.		
2.	HMG Grants Received.		
	Grants received from Class IX Vote 3 Subhead J6(1) 1992-93	3,744,169	3,423,094
3.	Operating Receipts		
	Receipts from registration fees	7,726,669	2,254,965
4.	Other Operating Payments		
	Rents & rates	265,590	257,563
	Maintenance, cleaning, heating & lighting	58,556	130,532
	Office supplies, printing, stationery	77,320	63,830
	Carriage & telephones	97,406	70,240
	Travel & subsistence	124,708	114,644
	Staff recruitment	3,648	8,447
	Specialist assistance	2,554	4,735
	Public relations	649,902	503,252
	Legal costs	67,754	64,763
	Staff training/health & safety	27,102	37,908
	Computer bureau	491,731	465,611
	Vehicle expenses	1,361	1,834
	Audit fee	6,050	5,730
	VAT	253,653	228,436
		2,127,335	1,957,527
5.	Other Receipts/Payments		
	Receipts		
	Pension contributions/transfers	39,480	77,400
	Bank interest	61,103	85,374
	Other interest	200	47
	Speakers' fees	476	850
	Sale of Goods	2,037	2,750
	Legal Costs recovered	12,081	3,328
		115,377	169,749
	Payments		
	Purchase of computer hardware/software	27,013	53,987
	Purchase of furniture & other office equipment	22,473	17,746
	Purchase of Van	–	7,319
	VAT	8,770	13,578
		58,256	92,630
6.	Appropriations Amounts surrendered to the Consolidated Fund via the Home Office during the year		
	Registration fees	7,512,764	2,276,902
	Other	115,377	170,013
		7,628,141	2,446,915
7.	Balance at Year End		
	Cash at bank	258,106	23,433
	Cash held at offices	323	377
		258,429	23,810

		1992/93 £	1991/92 £
8. Salaries and Employees			
(a) The salary of the Registrar is paid from the Consolidated Fund and is not therefore included in this account.			
(b) Corporate Managers			
The emoluments of Corporate Managers fell within the following ranges:		No.	No.
	£		
	30,001 – 35,000	0	1
	35,001 – 40,000	1	1
	40,001 – 45,000	2	1
(c) Staff Costs			
Salaries and Wages		1,374,919	1,240,506
Social Security Costs		97,982	87,829
Pension Costs		64,963	22,821
		1,537,864	1,351,156
The average number of persons employed by the Registrar during the year was as follows:			
Category		No.	No.
Corporate Management		3	3
Senior Staff		6	7
Other Staff		80	78
Occasional Casuals (full-time equivalent)		4	4
9. The Data Protection Registrar operates a non-contributory pension scheme to provide retirement and related benefits to all eligible employees. Retirement benefits are based on individual final emoluments. The scheme is funded on a pay-as-you-go-basis from Grant-in-Aid.			

E.J. HOWE CBE
DATA PROTECTION REGISTRAR

16 JUNE 1993

Certificate and Report of the Comptroller and Auditor General

I certify that I have examined the accounts on pages 105 to 107, in accordance with the Data Protection Act 1984, and the National Audit Office auditing standards.

In my opinion the financial statements properly present the receipts and payments of the Office of the Data Protection Registrar for the year ended 31 March 1993, and the balances held at that date and have been properly prepared in accordance with the Data Protection Act 1984, as directed by the Secretary of State, with the approval of the Treasury.

I have no observations to make on these statements.

John Bourn
Comptroller and Auditor General

National Audit Office

Printed in the United Kingdom for HMSO
[illegible]

HMSO publications are available from:

HMSO Publications Centre
(Mail, fax and telephone orders only)
PO Box 276, London, SW8 5DT
Telephone orders 071-873 9090
General enquiries 071-873 0011
(queuing system in operation for both numbers)
Fax orders 071-873 8200

HMSO Bookshops
49 High Holborn, London, WC1V 6HB
071-873 0011 Fax 071-873 8200 (counter service only)
258 Broad Street, Birmingham, B1 2HE
021-643 3740 Fax 021-643 6510
33 Wine Street, Bristol, BS1 2BQ
0272 264306 Fax 0272 294515
9-21 Princess Street, Manchester, M60 8AS
061-834 7201 Fax 061-833 0634
16 Arthur Street, Belfast, BT1 4GD
0232 238451 Fax 0232 235401
71 Lothian Road, Edinburgh, EH3 9AZ
031-228 4181 Fax 031-229 2734

HMSO's Accredited Agents
(see Yellow Pages)

and through good booksellers

ISBN 0-10-020953-X

780100 209534