Data Protection Act 1984

A Review by the Data Protection Registrar

Part B of the Fifth Report of the Data Protection Registrar June 1989

THE DATA PROTECTION REGISTRAR

Part B: A Review of the Data Protection Act 1984

Contents

B0. Introduction to the Review

Inevitably, data protection legislation has some complexities. It is a new form of law which deals with a rapidly developing, pervasive technology. Most importantly it requires new balances to be struck between different public policies. The legislation is bound to have teething troubles and it is sensible to study them to see if changes are necessary.

In previous Annual Reports I have promised to review the working of the Act at an appropriate time. There was little point carrying out any review until after 11 November 1987 when the Act came fully into force.

It is vital that a review of the Act should take account of the views and experience of a wide range of interested parties, including individuals and their representative bodies and also data users and their associations. Consequently I set up a consultation process to encourage both organisations and individuals to make their views known. I am grateful for the positive response I have received.

In planning this consultation, I made some assumptions:

— that the United Kingdom will wish to remain bound by the Council of Europe Convention and that there is therefore no question of abandoning data protection legislation;

— that experience so far has thrown up problems which may well call for changes either in the principal legislation or in subordinate instruments or in the administrative practice of my office;

— that much effort has been put into understanding the Act and the practical way is to seek to amend the Act in order to make it work better rather than to start completely afresh.

I also concluded that I should confine myself to those issues which are reasonably within my statutory competence. Data protection legislation does, however, raise a number of issues of public importance—such as the extension of regulation to manual records. I pointed out that if respondents wished to raise radical issues of that nature, those representations should best be addressed to Ministers and Parliamentarians rather than to me. But I undertook to pass comments of this nature, made in response to the consultation document, to the Home Office.

At the end of May 1988, I wrote to 310 organisations and individuals sending them copies of the consultation document ("What are your views") and inviting responses. Subsequently, many further requests for copies of the document were received. In all about 2100 copies were distributed to representative bodies, public authorities, government departments, consumer representative groups and individuals who were either data protection experts or simply interested members of the public.

Initially, responses were asked for by 1 August 1988. This clearly posed a difficulty for many respondents and the date was extended to 1 September 1988. The September postal strike then intervened to delay many of the responses. It was October before all responses had been received.

In all, 149 responses were received. They varied from, on the one hand, a short report that everyone in a particular industry seemed content and that the representative body had no comment to make, to, on the other hand, weighty strongly-argued cases for significant changes in the legislation from both individuals and representative organisations.

A number of individuals and public officials, not included in the 149, replied to the effect that they did not think they should make a formal representation to the Registrar. Those representative bodies and other organisations who replied explaining that an umbrella body was replying on their behalf are included in the 149. No attempt has been made to count all the separate organisations and individuals represented by those bodies which did respond.

Respondents were subsequently asked if they would agree to the publication of their responses and if I might pass copies to the Interdepartmental Committee, established by the Home Secretary in July 1988, which is also reviewing the legislation.

The Deputy Registrar and another member of my staff have read each of the responses several times. I have personally read all the responses. I should like to express my thanks particularly to my Deputy, Francis Aldhouse, for taking on the daunting task of analysing the views put forward and for his more general contribution to this review.

"What are your views?" looked at the issues relating to the Data Protection Act under nine headings:

— The Data Protection Principles

— The Register and Registration

— Supervision and Enforcement

— Rights of Data Subjects

— The Exemptions

— The Registrar's Powers

— General and Miscellaneous

— The Definitions, and

— Fundamental Issues

These same headings are used to describe both respondents' views (in Chapter 1 following) and the Registrar's views (in Chapter 2).

"What are your views?" contained a lengthy and detailed list of questions. In the course of the consultation, organisations asked for help in reducing this list. It did prove possible to provide a shortened list of questions which identifies the principal topics. That list is included as Appendix BA1.

To assist those who may be unfamiliar with data protection issues: a background to the Act is given in appendix BA2; the Data Protection Principles and their interpretations are reproduced in Appendix BA3; and a short glossary of terms is in Appendix BA4. Other appendices contain a list of those who responded to the consultation exercise (BA5) and tables showing some key responses (BA6).

It can be expected that this part of the Annual Report will be a matter for some debate. To assist referencing to points made, all paragraphs from now on are sequentially numbered.

Chapter 1: The Consultation—What you said

B1.1 Introduction

1. This chapter gives the general picture of responses made to the consultation document "What are your views".

2. That document contained a very large number of questions and not all respondents felt able to reply to each of them: the majority concentrated on selected questions chiefly about the Data Protection Principles and Registration. A few organisations commented that their members were content with matters as they were or that it was too soon to make proper comment.

3. Some questions raised in the consultation document are dealt with in this summary only briefly or together with another topic. But where the response to a question has shown distinct disagreement, the text tries to bring that out and show the weight of different opinions. Responses to some of the short list of key questions (see Appendix BA1) are also shown in table form in appendix BA6.

4. This general picture has to be a summary and some who have responded might fear that their contributions have been overlooked. All responses have been studied carefully and where the respondents have agreed I am making the responses available for inspection and research so that others may, if they wish, reach their own conclusions about the consultation and the response.

5. Readers must bear in mind that this paper reflects the views of the selection of organisations and individuals whom I chose to consult and those who were able to undertake what was often a considerable task to prepare a response. But, even so, I believe that the range of respondents and nature of their responses serve to give a fair indication of the range and strength of views about the legislation.

B1.2 The Data Protection Principles

6. Consultees were asked whether the Data Protection Principles or their interpretation needed amendment and whether all data users should have to comply with them. It was suggested that a general duty to comply with the Principles might make it possible to extend the exemptions from registration.

7. The response was overwhelmingly that there should be a clear duty on data users holding or using personal data to comply with the Data Protection Principles irrespective of registration. Equally strong was the view that the Principles—set out in Part 1 of the Schedule 1 to the Act (see Appendix BA3)—were a proper and sufficient code of practice.

8. Undoubtedly, the majority view is that the Principles should remain expressed in general terms so that they can be applied flexibly to a variety of different circumstances. Some individuals wished to see the Principles clarified and strengthened; one or two responses suggested a role for codes of practice to interpret the Principles in the context of particular industries.

9. A strongly held, but distinctly a minority view (expressed notably by the Finance Houses Association and the Advertising Association) was that no change should be made to the present structure of the legislation. They linked this view with a point made by some that there was as yet insufficient experience on which to base comment and any review would be premature.

10. A further minority take the view that the effect of Section 2(2) of the 1984 Act is that the Data Protection Principles do apply to all users, it is merely that the Act only provides an enforcement system in respect of registered data users. Those holding this opinion take the view that this lack of enforcement power in some cases is a defect which should be remedied.

11. A number of respondents wished to see no changes to the interpretation provisions of the Principles (see Appendix BA3). On the other hand, others proposed a variety of changes. Some were critical of the partial exemption from the First Principle for information obtained or disclosed under statutory authority. Many asked for greater precision in the Eighth Principle which it was suggested might be achieved by adding interpretation provisions to that Principle.

12. There is clearly a feeling among data users that the principal concern of individuals is not that information might be kept or used but that it should be confined to the organisation and purpose for which it was provided. That echoes the comments of individuals, and consumer and civil liberties bodies. This view probably lies behind the proposal made by a number of respondents—including the Confederation of British Industry (CBI)—that the interpretation of the Third Principle should be amended by deleting references to disclosures. The consequence would be that a disclosure of data would not be deemed to be compatible with the purpose for which the data were held merely because a data user had registered it.

B1.3 The Register and Registration

13. Briefly, the consultation document asked whether the present registration system fulfilled the correct purposes; whether the register could be simplified; whether more people should be exempt from registration; and whether there should be administrative flexibility to provide special registration arrangements for partnerships and some other special cases.

14. The range of responses on the value and nature of the registration system was very wide. Some—notably the chartered accountancy bodies—took the view that registration should be abolished and resources concentrated on enforcing the Principles on all data users holding personal data. On the other hand, those such as the Advertising Association would make no change to the present arrangements because they argue that the register serves as notification to the public of the fact that personal data are held, what those data are and the purposes to which they are put.

15. The general response, however, was clear. The registration forms and the standard categories for purposes and data produced by the Registrar had caused difficulties, but were generally acceptable. Some found the structure inappropriate to the way they wanted to describe their activities. Small organisations found the greatest difficulty although this had been partially alleviated by the short registration form published by the Registrar. However, respondents believe that the resulting register is complex and of little value to a data subject or anyone else examining a register entry to try to find what a particular data user might be doing.

16. Respondents do believe that a register is useful to the Registrar to provide a list of those who should be complying with the Principles and therefore at whom enforcement should be directed. Respondents also recognise that the enforcement of data protection entails public expenditure and most accept registration as a means of raising the necessary revenue. It was suggested that if the objective of a register is to tell data subjects which data users hold personal data then a much simplified register—even a mere list—would be sufficient.

17. There was considerable—though not universal—opposition to the idea that organisations should be exempt from registration on the grounds of size alone. It was thought that the sensitivity of the data held and the uses made of it have little relationship to the size of the data user organisation.

18. However, many put forward various proposals for two-level registration. Those identified as carrying out non-sensitive activities might register in the simplest form—perhaps with just name and address; the more sensitive activities or data would require a greater level of detail. The non-sensitive cases might also remain on the register for a longer period without renewal. Several respondents mentioned favourably the recent Irish legislation which imposes a general duty on data controllers to comply with rules similar to the United Kingdom Data Protection Principles, but only requires a limited group of data users to register.

19. Another popular proposal was for almost universal registration at a very simple level—name, address and possibly some indication of the broad purposes or activities of the data user. There were, of course, variations on this theme, but the general picture is clear. This was seen: as helping small

organisations register; as consistent with the view that all should be bound to comply with the Principles; as providing an enforcement list for the Registrar; and as providing the means to raise revenue. Many expressed the hope that such a simplified system would eliminate the need for frequent changes to register entries.

20. Exemptions are considered later in more detail, but the predominant view has already been mentioned — namely size is not of itself a justifiable criterion. On the question of the registration fee, the predominant view was that the present flat rate should remain.

21. The suggestion for administrative flexibility caused disquiet with some respondents. But others who have had the experience of discussing arrangements for registering partnerships, churches and groups of companies were sympathetic to special schemes to deal with those and similar cases. There seemed to be a view that these schemes would be more acceptable if registration were simplified in one of the ways commonly proposed.

B1.4 Supervision and Enforcement

22. A variety of questions were posed. Principally, people were asked whether the powers of the Registrar were sufficient and whether he should carry out systematic inspections. The consultation document also invited views on criminal penalties, the question as to whether individuals should be able to apply directly to the Data Protection Tribunal and the extent of that Tribunal's jurisdiction.

23. On this topic, the response of many was that it was too early to give proper comments. This was because the provisions of the 1984 Act had not been properly tested, few prosecutions had been brought and the Tribunal had not yet sat.

24. Those who favoured a duty on all to comply with the Principles and radically simplified registration tended to favour some extension of the Registrar's powers to obtain information. Some supported the proposal for the Registrar to conduct systematic inspections after the manner of factory or health inspectors; on the other hand, some were of the view that no change at all was required. Among representatives of data users there was clearly a feeling that systematic inspection would be invasive and disruptive, and could not be justified by sufficient evidence of widespread problems. However, some of these bodies suggest that the Registrar should have the power to conduct inspections where he had cause for suspicion and a power to demand information, perhaps by a process akin to that in the recent Irish legislation which allows the Irish Commissioner to serve a notice requiring information to be given to him.

25. On penalties, the general view was that there is no sufficient ground to change the present structure. Some felt that imprisonment should be available for extreme cases; and conversely several respondents suggested that there should be no criminal sanction for any breach of the Act. One respondent defending the present structure indicated that direct enforcement of the principles by criminal penalty would be well nigh impossible given the generality of their drafting and the heavy burden on a prosecution.

26. There was a similar variety of response to the issue of whether individuals should have the right to take direct proceedings against a data user for breach of one of the Data Protection Principles, rather than complain to the Registrar as at present. Perhaps the typical view would be that individuals should not go straight to the Data Protection Tribunal, but should perhaps be able to appeal against a decision of the Registrar not to take enforcement action. The Tribunal could then consider whether there had been a breach of Principle and whether any remedy was appropriate.

27. Questions relating to the role of the Data Protection Tribunal were divided in the consultation document between the section on Supervision and Enforcement and the section on the Rights of Data Subjects. The general response to all these questions is summarised here. The overwhelming view was that there must be recourse to the ordinary courts to settle points of law. On the issue of whether the jurisdiction of the Tribunal should be extended to hear cases brought by individuals under the Act as it currently stands (eg. compensation claims), views were mixed. Certainly some favoured building up the role of the Tribunal to allow it to develop expertise in all matters of data

protection. A specific point was the desire by at least one representative body to have a forum before which it could bring doubtful issues of law when there was no other opportunity for litigation. Organisations could act with greater certainty when the law had been declared without having to run the risk of a legal disagreement with the Registrar and possible prosecution or enforcement proceedings.

28. Finally, a number of respondents felt that it should be possible to prosecute government departments. They could see no reason why government departments should be treated differently from other data users.

B1.5 Rights of Data Subjects

29. The questions under this heading dealt in part with the role of the Tribunal and those responses were summarised in the previous section. Questions were also asked about the extent of the rights of individuals and about subject access.

30. These issues distinguished those who replied from a consumer or civil liberties standpoint from those responding for organisations representing data users. On the one hand, there are views that data subjects should have a general right to enforce the 1984 Act and that compensation should be payable for pure distress; on the other hand are those who see no argument for any change and doubt whether there is any evidence of abuse or hardship to individuals justifying change. This division of opinion is emphasised by that organisation which in its general comments denies that the purpose of the legislation is "principally conferring individual rights" and asserts that, "the Act should not be used as a means of introducing through the back door a legal right of privacy ...". The neutral positions were those who had no view to express or felt that there was insufficient experience to comment.

31. Subject access was another matter. Many commented on the limited use made of the right—at least so far as it affected any single data user. The predominant view among data user representatives was that a fee should be chargeable to discourage frivolous requests, but that the maximum fee chargeable as a result of multiple register entries should be restricted. Data subject representatives were more critical of the fee and the likelihood of its discouraging legitimate subject access requests.

32. Data subject representatives were on the whole enthusiastic about logs of sources and disclosures. But some recognised the strength of arguments put forward by data user representatives that as a general rule the maintenance of such logs would be impractical. The library representatives argued how unrealistic it would be to log disclosures from bibliographic catalogues.

33. There was a substantial response to the Registrar's request for solutions to the dilemma that arises when data are withheld under a subject access exemption, but the data subject is not told that the exemption has been used. Some suggested that this dilemma was nowhere near as serious as might be thought and that, except in a very few cases, individuals should be told that a subject access exemption had been relied on to withhold data. Others recognised the problem, but were unable to propose a solution. The typical solution—although opposed by some—was that data users should report their use of these exemptions to the Registrar so that he might check on the propriety of using them.

34. Some strong representations were made about the importance of Section 21(4)(a) of the Act. This Section allows a data user to ask for the assistance of a data subject to locate data when answering a subject access request. There was a strong view that without this assistance answering subject access requests would be "simply not practicable".

35. Sections 21(4) and 21(5) of the Act allow a data user to withhold information from a data subject which relates to another individual who can be identified from the information or identified as the source of information. The Registrar takes the view that the test of whether the third party is identifiable is

an objective test; so any special knowledge, which would enable the data subject to identify the third party whereas everyone else could not, should be ignored. Some expressed the view that the Registrar's interpretation of the Act was mistaken. A number of organisations are of the view that information about third parties should be withheld if the data subject could identify the third party from his special knowledge and that the Act should be amended to this effect if that is not already its true interpretation. On the other hand a quite strong view was put that this provision should not be relied upon to hide the names of professional informants and advisers.

36. A further proposal was that data subjects should be required to send their subject access requests to the address specified in the register. The Registrar takes the view that this is not a compulsory address and that the individual has a choice about how to make his request.

B1.6 The Exemptions

37. This topic is closely related to the role of the Data Protection Principles, proposals for registration and the rights of data subjects. Many people answered questions about exemptions from the whole Act by suggesting either a system of almost universal but simple registration, with the consequent repeal of the registration exemptions, or a duty on all data users to comply with the Principles linked to extended exemption from registration.

38. There was widespread sympathy for the problem of small organisations or individuals carrying out non-sensitive activities. Nevertheless, the predominant view was that the size of an organisation alone was not a proper criterion for exemption from registration. That view was perhaps less strongly held by those proposing some form of two-level registration or linking exemption from registration to an enforceable duty to comply with the Principles. Many supported the accounts and payroll exemption from registration but believe that it should be widened to make it more readily available. A related idea was that data used only internally within an organisation might be exempt from registration.

39. There was some support for the suggestion that a data user processing with the permission of the data subject and complying with the Principles should be exempt from registration. But there was a cogently expressed counter-argument that such an exemption raises difficult issues about the validity of the consent and it was suggested that there are more straightforward ways of easing the burden on non-sensitive data users.

40. There was considerable opposition to any special exemption for the media or journalists as such. The media bodies did, however, argue for an exemption from subject access to the journalists' computerised notebooks. There was some support for the media view that published material should be exempt. Supporters of the exemption seem to have in mind data put freely into the public domain by the data subject himself or broadcasts such as a play in which the data subjects are the author, actors and others involved in the production. Opponents are thinking of journalistic activities leading to publication with no cooperation or consent of the data subject.

41. Very strong views were expressed by librarians and information specialists about the inclusion of bibliographic data within the scope of the Act. Support was also expressed for excluding other categories of data that might be considered to be in the public domain such as stocklists containing the names of individual authors, creators or sponsors. One body suggested a complete exemption for all public domain information such as the electoral register.

B1.7 The Registrar's Powers

42. In the context of enforcement and investigation, some respondents declined to comment on the extent of the Registrar's powers because any problems relating to them were not within their knowledge. Others expressed this view more strongly by saying that the consultation document gave no evidence for extending the powers. On the other hand, some strong representations were made that the Registrar should have express powers to investigate, to obtain information and to inspect. The general tenor of these views was summarised in section B1.4.

43. Opinions were divided, but a majority thought that the Registrar should be able to assist individuals to bring data protection cases to court. At least one representation was of the view that the Registrar could currently do that. The minority opinion sometimes went to the extent of saying that the Registrar should not have such a power because it would show bias against data users.

44. On the question of reviewing the legislation, three opinions are clear. A few hold that this is a political matter entirely for Ministers and Parliament. Others say that the Registrar seems to be able to carry out his present exercise without any specific power, in which case it is doubtful whether any change is required. The third group believe that the Registrar should have a duty akin to that of some other fringe bodies to keep the legislation under review and to report on his proposals.

45. There is a wide difference of opinion about codes of practice. One view is that statutory codes of practice should be developed to regulate specific industries. The codes would be detailed applications of the principles. Some take the view that this would be the right longer-term course even though it might be premature until more experience has been gained of the working of the legislation.

46. The opposite view put forward is that the principles are flexible and capable of being applied by the courts to a wide variety of circumstances, interpreting words such as fair, accurate and necessary as they commonly have to do in other cases. This view sees a limited role for codes of practice.

47. A middle opinion believes that codes of practice could be useful but that their status should be clarified. Predominantly, but not universally, the opinion is that codes should be developed by trade and professional bodies, that there should be a formal procedure for endorsement by the Registrar, and that such a formally endorsed code should have a similar status to the Highway Code in any data protection legal proceedings. Thus compliance with or a breach of the Code would be taken into account by the Tribunal, but a breach of the Code would not itself be a breach of Principle or any other enforceable provision of the Act.

B1.8 General and Miscellaneous

48. Under this heading, the Registrar asked about three topics: the practice, of employers and others, of making individuals exercise their right of subject access for vetting purposes; the introduction of administrative flexibility by statutory instrument; and Section 39 of the 1984 Act which deals with data held and services provided outside the United Kingdom.

49. The overwhelming view was that it was an abuse of the Act to make someone use his subject access rights so that the information could be seen by someone such as a prospective employer. Most who responded thought it should be prohibited and made a criminal offence. A minority group put in a plea for the legitimacy of vetting prospective employees and licence holders in what they considered to be particularly sensitive areas. The local authority associations are especially concerned about the previous criminal records of taxi drivers.

50. There was a limited, but largely favourable, response to the suggestion of giving greater administrative flexibility to be exercised by statutory instrument. That would enable special rules to be developed to deal with the registration of partnerships, groups of companies, churches and other practical problems met in applying the registration system. A few were outspokenly critical of the use of subordinate legislation to give that flexibility. They suspect that its use might have the effect of weakening data protection control.

51. The response on Section 39 (the application of the 1984 Act to overseas held and used data) was uncertain. Those who responded tended to agree that clarification would be valuable.

52. A special point made by a number of respondents concerned the exercise of subject access rights by the mentally disabled and children. There was a plea for a special order to resolve the position of the mentally disabled. Views were expressed about the uncertain effect of the law relating to children and subject access in England, Wales and Northern Ireland. A request was made for the law to be clear on the age at which the right of subject access could be exercised. A County Council pointed out the anomaly likely to arise as a result of the proposals for access to school records under the Education Act 1980. These rights of access cannot be exercised by a pupil until 18 years of age, but the same pupil, if of years of discretion, can exercise rights of subject access to similar records under the Data Protection Act.

B1.9 The Definitions

53. Comments were invited on all the definitions in the 1984 Act, and certain points were raised specifically.

54. Very varied views were expressed. The general impression is one of caution on the part of commentators; a reluctance to comment in the absence of clearly identified practical problems and an underlying feeling that, as the Institute of Personnel Management put it, "...for the layman, the definitions contained in the Act are excessively complex and legalistic". The cautious approach was well expressed by the British Bankers Association:

> "... unnecessary tampering should be avoided, since the complex and inter-related nature of the Act could result in minor change having unforseen and retrograde effects elsewhere."

55. Others did set out about commenting on most definitions and proposing detailed changes. One view was that the definitions should be simplified to correspond to the wording of the Council of Europe Convention.

56. Most were content with the definition of "data". They believe there should be a definition in the Act. They disagreed about whether or not data should be information in a recorded form. But the problem of transfer overseas in a non-recorded form was recognised. Some saw this as a difficulty and others not.

57. Some believe that all personal data should be subject to the Data Protection Principles, but others argue that the right of subject access could not be exercised in relation to transient non-recorded data and such data ought therefore to be outside the scope of the Act.

58. There was limited comment on the phrase "by equipment operating automatically in response to instructions given for that purpose". Those who responded believe that it does properly restrict the scope of the legislation. One comment expressed concern that this was thought to confine the 1984 Act to the stored program concept. There was some support but no widespread enthusiasm for applying the restriction to processing rather than data.

59. There was some—but not unopposed—sympathy for narrowing the definition of personal data by excluding that information which could be said to relate to a business or which had been placed in the public domain. Respondents were reluctant to propose ways of achieving this redefinition.

60. There were strongly held views about "opinions" and "intentions". A few maintain that there is a clear distinction which should be maintained. Many believe the distinction is unworkable and that no special exemption should apply to intentions. Those who pressed for the special provision in the 1984 Act relating to intentions do understand how the same matter can be expressed as opinion or intention and how it is often unclear which is the case. They simply argue for a means of protecting personnel succession planning information from subject access.

61. Most seem content with the phrase "relates to a living individual".

62. There is uncertainty about the value of requiring, in the definition of a

"data user", that data form part of a collection. Some agree that the requirement should be abolished.

63. Different views were expressed about "jointly or in common". Those who responded from a non-legal background tended to reply more in favour of the words than did the lawyers. The general tenor of the comments seems to be that there should be a means either of identifying a single data user or of saying that someone is a data user even when control is shared, but that it should be done more simply than by using the phrase "jointly or in common".

64. Respondents were concerned about the meaning of "control". What is not clear is whether the word can be more precisely defined.

65. There was only limited comment on the definition of "computer bureau". Most seem content. Some concern was expressed that an organisation might fall outside the definition because it carried out further activities not mentioned in the definition. "Agent", both here and elsewhere, provoked firm views. Generally, respondents argue that "agent" should carry a broader meaning than that which the Registrar believes it has. On the other hand, disclosures to maintenance organisations should be within the non-disclosure exemptions.

66. There was some comment on "processing". There was disagreement about whether it should be extended to include "storage" or at all. There was some support for extending the list of activities to include "transmission", and also "inputting", because the present definitions tend to imply that data already exists in an automated system.

67. "Text preparation" provided much comment. Views varied widely from the practical approach that the current exclusion seems to work in practice and should be left alone, to the far reaching view that the exclusion is unintelligible. Generally, respondents consider that straightforward word-processing should be excluded from the scope of the Act. There was also some support for excluding filed electronic mail.

68. The Registrar takes a broad view of what is meant by processing "by reference to the data subject"—including all processing directed towards an individual whether the reference used is a name, an identifier, or simply a characteristic. The consultation document suggested that the meaning of the phrase could be clarified, perhaps by expressly including processing by reference to categories of data subject. The issue is whether the legislation should control personal data which is analysed to look, for example, for all red-headed men or all the mentally ill or similar groups identified by characteristic; the result of such a search being a list of names of a particular sort of person. Some respondents clearly and distinctly disagree with the Registrar's view of what is meant by processing "by reference to the data subject" and would oppose extending the definition of the phrase to include processing by reference to classes of individual. Others simply support the proposal to clarify the definition. There are also some who agree with the Registrar's view of what is meant by the phrase. The British Computer Society take a half-way position and suggests that processing by reference to classes should only be included where sensitive data are concerned.

B1.10 Fundamental Issues

69. Some people chose this section to make a variety of miscellaneous points, the tenor of which has been covered in earlier chapters. The principal fundamental issue raised was the extension of the Act to manual records. Respondents recognised that this was not strictly relevant to a consideration of the 1984 Act, but some felt that the exclusion of manual records was increasingly anomalous particularly in the light of recent Access to Files legislation. However, others were opposed to any extension to manual records.

70. A second issue raised by a small business organisation was that data relating to artificial legal persons should be protected just as much as personal data, because in the case of the sole trader or the one-man company it was difficult to make a reasoned distinction between the personal and the business data.

B1.11 Overview

71. The Registrar specifically wrote to 310 organisations and individuals sending them copies of the consultation document "What are your views?". Most of the organisations represented trade sectors and similar groups. Some were deliberately chosen to represent the "consumer interest". A number of individuals with whom the office has had contact were also written to. Subsequently, requests for copies of "What are your views?" were received from many other organisations and individuals.

72. One hundred and forty-nine organisations and individuals have responded. That number includes those representative bodies who wrote to say that they were making a joint-submission with another organisation or were joining with others under an umbrella body. The number does not include those regulatory bodies who wrote to say that they did not think they could assist the Registrar in this review; nor does it include the individuals who wrote declining to respond.

73. Some organisations have clearly addressed the problem from their own standpoint as a data user and have largely confined their remarks to comments on the registration process; they have not usually considered the position of data subjects. Other organisations, including some representative bodies, have expressed a general data user view which expressly or implicitly deals with what is seen as the burden of the legislation on data users and correspondingly gives limited attention to the viewpoint of ordinary citizens. A third group of representative bodies, which would commonly be seen as acting for data users, has sometimes expressly sought to look at both data user and the data subject point of view. Representations from individuals tend to reflect their personal or professional position and experience. The few bodies representing the consumer tend to give expressly—often trenchantly—a data subject view.

74. Consequently, it is doubtful whether conclusions can be drawn from this consultation merely by counting the number of responses favouring a particular view. A judgement will have to be exercised about the objectives and constraints of the legislation and the appropriateness of the standpoint adopted by particular respondents. There are, however, some themes where the general tenor of the response is very clear.

75. The Data Protection Principles should apply and be enforced on anyone who uses personal data. It is perhaps premature to make major changes to the Principles and their interpretation, but the interpretation of the Third Principle should be modified so that disclosing data is not treated as compatible with the purpose for which it is held merely because the disclosure is registered.

76. It is right to have a registration system, but the present arrangements are burdensome, and are unhelpful to data users and data subjects alike. There is sympathy for small data users, but size is not a proper reason for exemption. A radically simplified register would be favoured. This might be of a simple almost-universal nature; or on a "two-tier" basis where more sensitive activities or personal data are registered in greater detail; or be restricted to certain categories of activity or personal data.

77. Individuals should have some right to appeal to the Data Protection Tribunal which could have a widened jurisdiction but should not exclude the

courts. The Registrar should be the principal means of enforcing the Data Protection Act. He should concentrate effort on securing compliance with the Principles. He should not visit data users routinely and regularly, but he should be able to carry out inspections and obtain information when appropriate.

78. There should be a subject access fee to discourage frivolous applications, but there should be an overall maximum.

79. Source and disclosure logs cannot generally be kept.

80. The practice of making an individual use his subject access rights to let a prospective employer see if he has a criminal record should be stopped.

81. Codes of practice can be useful, but it is too early to codify the proper practice of trade sectors, even if it were theoretically possible. There should be a formal approval process for codes so that compliance with them or breach of them is taken into account by a Tribunal considering an enforcement or similar notice.

82. The definitions need revising and clarifying in places. A particular plea was made by the library sector to exempt data such as that in library catalogues. Great care should be taken not to make unintended changes by ill considered meddling.

83. It is still very early in the life of the legislation to comment on the need for changes and most people have settled down to complying with the 1984 Act as it is.

Chapter 2: The Registrar's views

B2.1 Introduction

84. This part of my Annual Report puts forward suggestions for possible changes to the Data Protection Act 1984. They are framed as a series of recommendations which Ministers and Parliament may wish to consider if they decide the Act should be amended.

85. The objective of the recommendations is to:

— clarify the meaning of the Act;

— simplify the application of the Act;

— make the protection the Act offers to individuals more effective;

— encourage attention to be directed to the issues of greatest concern.

86. In making these recommendations I am grateful and indebted to those who responded to the consultation document—"What Are Your Views?". Many people put a great deal of time and thought into the responses received. The bulk of those responses are from bodies each of which represents many data users or individuals. They are rich in ideas born of practical experience with the Act.

87. However, the views put to me cannot be the only matters to take into account. I must also have regard to the working experience of my office and the results of research projects undertaken. The way in which data protection legislation is developing in other countries also has some influence.

88. My office has carried out research over the last few years into public attitudes. The results show a consistently high level of concern about privacy. "Keeping personal information or details private" is the aspect of privacy causing most concern. "Organisations building up files about me" is also of significant concern. More than two thirds of respondents are "very" or "quite" concerned about the amount of information kept about them by organisations.

89. The research also shows that a large majority of the public consider the rights specifically conferred by the Act — to see data and have it corrected — to be very important. There is, in addition, as much support for other "rights", such as to be told where information was obtained and to whom it might be passed and to have oneself removed from lists or files.

90. Some of the views available to me will, of course, oppose each other and I have sought to suggest appropriate balances. I have in mind: the legitimate interests both of individuals and data users; the objective of achieving a proper and practical inter-relationship between data protection and other public policies; and the need to meet the objectives and requirements of the Council of Europe Convention.

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

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

93. The "general rules" which the Convention lays down are largely incorporated in the Data Protection Principles which appear in the United Kingdom Act. These Principles are, in my view, the heart of the Act and the key to effective data protection. Whilst there are roles which can be played by registration, too much weight has been given to this aspect of the Act's requirements.

94. That view seems to be shared by those who responded to the consultation document. The two key observations were:

1. The Data Protection Principles state good practices which all data users should be required to follow.

2. Registration is too complex and all embracing and should be simplified.

95. Those consulted overwhelmingly support these two views. The support is not, however, unanimous. A few of the data user representative groups do not wish to see any changes made to registration or indeed to the Act as a whole. I have followed the views of the majority in making recommendations.

96. The recommendations concentrate on the two key views. If amendment of the Act is to be considered, then it seems better to start with any more fundamental considerations first. I am also mindful that there has not yet been the opportunity for the courts to determine the detailed meaning of the law.

97. However, it is important when considering any changes to the Act to understand its structure; in particular, the detailed way in which registration links into many different parts of the Act. Changes in registration have "knock on" effects on such matters as enforcement and on the Data Protection Principles. The recommendations take account of changes which are consequent on a proposed change in the registration method.

98. The consultation document ("What Are Your Views?") looked at the issues relating to the Data Protection Act under nine headings:

— The Data Protection Principles

— The Register and Registration

— Supervision and Enforcement

— Rights of the Data Subject

— The Exemptions

— The Registrar's Powers

— General and Miscellaneous

— The Definitions

— Fundamental Issues

99. These headings have been used to report the responses to the consultation and I have followed a similar pattern in putting forward my own recommendations.

100. A fundamental question is the approach to be taken in legislation of this type. Should it be prescriptive; or should it set requirements and objectives in general terms, leaving the prescriptive detail to arise from the determination of

particular cases? I favour the second approach and the recommendations are made on that basis.

101. Whether the Act should be amended and, if it is, the weight which might be given to the recommendations made, are matters for Ministers and Parliament. I shall be pleased to explain and develop these recommendations if this is helpful. I shall also continue to give my advice, as required, to the Home Office Interdepartmental Review Committee on Data Protection.

102. The Act has not been fully in force for long and in any interim period before Ministerial or Parliamentary decisions there could be a continuing consideration of experience and opinion to see if the recommendations might need modification. If adopted, they would, in any case, need putting into statutory form.

B2.2 The Data Protection Principles

103. I agree with the majority of respondents who say that the Data Protection Principles are a good code of practice for information handling. I also agree that the Principles, as currently written, are sufficient without modification. However, as some respondents have suggested, the interpretations of the Principles could usefully be revised. The adoption of the restricted registration system recommended later will throw greater weight on the Principles. Interpretations which assist in applying the general statements in the Principles will be helpful.

104. In this section, therefore, I suggest leaving the Principles themselves as they stand but put forward a number of possible amendments to the interpretation clauses. Some of the amendments are pertinent to more than one Principle and I deal with these first before considering those amendments specific to particular Principles. The Principles and their interpretation are set out in Appendix BA3.

(a) Changes Affecting More Than One Principle

105. I later suggest some changes to the registration system. These changes mean that less detail will be registered as to data users' activities. The effect is that data users would no longer be able to satisfy Principle 3 (regarding the compatibility of uses and disclosures of personal data with the purpose for which the data are held) simply by the details they enter in the Register. Nor would the interpretation of Principle 2, which also refers to the Register, any longer make sense. Consequently, the current interpretation of those two Principles would need to be struck out.

106. Principles 2, 3, 4 and 6 refer to the purposes for which personal data are held. There is a difficulty in the practical application of the Act in determining for what purposes personal data are actually held. This is particularly difficult when the Act also refers to purposes for which personal data are used.

107. It would be helpful to have some guidance as to matters to take into account in determining whether personal data are actually held for a purpose or not. I take the view that the best guide to this is the purpose for which the information was originally obtained by the data user.

108. I therefore recommend that an interpretation should be added to Principles 2, 3, 4 and 6 indicating that: in determining whether personal data are held for a purpose, regard shall be had to the purpose or purposes for which the information constituting the personal data was obtained by the data user.

109. Principles 4 and 6 also have another problem in common. It is difficult to apply either of these Principles without having regard to the circumstances of the individual or invididuals who are the subjects of the personal data. Yet the Principles themselves make no reference to data subjects but only to purposes for which the personal data are held.

110. I therefore recommend that these two Principles should each have an interpretation added to the effect that in determining whether personal data are (Principle 4—adequate, relevant and not excessive) (Principle 6—not kept for longer than is necessary) regard shall be had: to the circumstances of the indi-

vidual or individuals who are the subjects of the data, or to whom the data are related (whether by the processing carried out by the data user or otherwise); and to the uses which may be made of the data in relation to those individuals.

111. Having made points which are common to more than one Principle, I now consider each Principle in turn to see if modifications or additions to the interpretation provisions might be appropriate.

(b) The First Principle

112. This Principle requires that information which is to be contained in personal data shall be fairly and lawfully obtained and that personal data shall be fairly and lawfully processed. Much in this Principle depends on the interpretation of "fairness" both for the obtaining of information and for the processing of data. It is not entirely clear what is meant by "fairness". This uncertainty will be resolved by the courts as the legislation comes to be tested more regularly. However, the interpretation paragraph 1(1) of the First Principle does give some guidance as to fairness in obtaining information by referring to whether any person was deceived or misled.

113. Another circumstance in which interpretative guidance would be helpful arises in those cases where a data user is obtaining information in order to supply or make it available to others.

114. In other circumstances the Third Principle may afford an individual some protection against widespread and indiscriminate disclosure of information about him, because it provides that uses and disclosures of personal data must not be incompatible with the purpose for which the data are held.

115. However, where the data are held for the purpose of making disclosures the protection of the Third Principle is lost. I recommend that this is overcome by adding into the present interpretation paragraph 1(1) of the First Principle a phrase indicating that: in assessing whether information is fairly obtained, regard shall be had as to whether an individual was given any choice as to the uses or disclosures to be made of the information.

116. The Data Protection Act sensibly incorporates some rules for avoiding conflict between this Act and other statutory provisions. Two of those rules are set out in interpretation paragraph 1(2) of the First Principle. As a consequence, information is deemed to be obtained fairly if it is obtained from someone authorised or required to supply it by statute or international agreement. Also, in assessing whether a data user obtained information fairly, no account is to be taken of a disclosure similarly authorised.

117. With these rules it might be expected that there would be counterbalancing rules in other legislation setting out appropriate codes for the obtaining of information in those specific circumstances, but that is not the common practice. In any case, there is a substantial body of pre-existing legislation which does not address these issues at all.

118. I would argue that this complete exemption for those acting under statutory authority is too sweeping and may licence practices which on their merits would be unacceptable in other circumstances. Considerable weight must be given to the fact that someone is acting with statutory authority, but it is difficult to see why this should automatically be an overriding consideration.

119. I recommend that the proper course would be to amend the interpretation paragraph 1(2) of the First Principle so that acting under statutory powers raises a presumption that information has been fairly obtained, but a presumption which could be rebutted on the facts of the particular case where it could be demonstrated that the application of the First Principle would not be likely to prejudice the statutory purpose for which the information was being obtained.

120. "Processing" is defined by the Act as a set of technical operations—namely amending, augmenting, deleting or rearranging data or extracting information constituting data. These operations make no reference to the purpose of the activity or the subsequent use of the data. But if "processing" is to be judged as fair or unfair, it seems difficult to make that assessment without looking at the consequences of the processing for an individual data subject. This approach to judging fairness comes close to dealing with the issues of incompatible uses and disclosures dealt with in the Third Principle. Consequently, a difficult distinction has to be drawn in practice between the proper area of these two Principles.

121. To resolve this difficulty I recommend that a paragraph should be added to the interpretation provisions for the First Principle. This should provide that, in determining whether information is processed fairly, regard shall be had to the purpose of the processing and the forseeable consequences of the processing for the individual data subjects whose data are being processed.

(c) The Second Principle

122. The Council of Europe Convention and much of the discussion of data protection involves the idea that data should be held for specified purposes and used only in ways compatible with those purposes—this is often called the finality principle and it is set out in the Act in the Second and Third Principles.

123. I have dealt in part (a) of this section with a proposed interpretation to help to assess whether personal data are held for a purpose. I have also dealt with the effect of proposed changes in the registration system.

124. There remains the issue as to whether a purpose, however described by a data user, is sufficiently specified. In this respect, respondents have suggested that data users would find it helpful if the Registrar continued to publish a list of recommended purpose descriptions. I also have in mind that whether a particular purpose description has been appropriately specified ought to depend on the reasonable expectation of those providing the information as to the uses to which that information will be put.

125. I recommend therefore that there should be a paragraph in the interpretation of the Second Principle indicating that: in determining whether a purpose is sufficiently specified regard should be had to: (i) whether the purpose is in a form approved by the Registrar; and (ii) the circumstances in which and purposes for which the information constituting the data were obtained.

(d) The Third Principle

126. On the face of it this Principle suggests that a judgement will be made on the merits of whether personal data are used or disclosed in a way incompatible with the purposes for which they are held. In practice that is not so, because the interpretation deems uses and disclosures to be compatible—however unlikely or unreasonable—provided that they have been registered.

127. There has been considerable opposition to this deeming provision—particularly as it relates to disclosures—from a variety of groups. Again a balance has to be struck between the desire of those holding personal data to be certain that their uses and disclosures are lawful and, on the other hand, the protection of individuals.

128. In part (a) of this section I have explained that the later proposals for a revised registration system would necessitate striking out the present interpretation. However, regardless of whether the registration system is changed or not, I believe the present interpretation provision bends too far in the direction of certainty for data users. It permits, by registration, practices which many,

including business representatives, would believe to be unacceptable. I would recommend in any case that the best course would be to delete the present interpretation provision entirely and leave matters to be assessed on their merits, if necessary by the Data Protection Tribunal and the courts.

129. The Act contemplates a distinction between the purposes for which data are held – the principle purposes – and the purposes for which the data are subsequently used – the subsidiary purposes. A difficulty with the practical application of the Act in general, and this Principle in particular, is distinguishing between the purpose for which data are held and the uses to which the data are put. In part (a) of this section I have recommended an interpretation which should assist in determining the purpose for which the data are held.

130. It would also be valuable to have some guidance as to whether personal data have been disclosed in a manner incompatible with the purpose of purposes for which they are held. I recommend that a further interpretation paragraph should therefore state that, in determining whether a disclosure is incompatible or not, regard shall be had to the purposes for which the data are to be used by the person to whom they are disclosed.

(e) The Fourth Principle

131. This Principle requires data to be adequate, relevant and not excessive. There is no interpretation provision. On first approaching the Principle, there is a tendency to look at whether the personal data are adequate, relevant or excessive in relation to the circumstances of an individual who has brought a complaint. However, the Principle only says that these conditions should be related to the purpose for which data are held. Those purposes must often be cast in very broad terms.

132. I have concluded that this Principle can at present only work justly if data users are required to specify very finely detailed purposes. That is probably overburdensome and unnecessary. I have consequently recommended an alternative approach in part (a) of this section. This sets out an interpretation provision which will bring the circumstances of individuals into countenance.

(f) The Fifth Principle

133. This Principle requires data to be accurate and, where necessary, kept up to date. There are practical problems in applying this Principle, but only such as arise when interpreting any general words such as "accurate" and "necessary". The proper course in my view is to allow their meaning in the context of this Act, to be settled by the courts.

134. The current interpretation of the Principle raises a problem in that personal data marked as received from a data subject or a third party and accurately recording the information provided by the other person are (subject to certain conditions) not to be treated as inaccurate. This negates a data subject's right to compensation if he or she is damaged by these data because, in fact, they prove to be inaccurate.

135. Here again the legislation strikes a balance between the rights of people to collect and use information without undue legal restriction and the damage which inaccuracy can inflict on individuals. The legislation includes a procedure to enable a data user to protect himself from having to act as a guarantor of the complete accuracy of everything other people tell him; but the Act also provides a means (in Section 24) by which an individual can apply to the court to have inaccurate data rectified even if it has been marked as received from a third party. I see the good sense of these arrangements, but on the other hand I am conscious that inaccuracy, even if unintentional, can cause considerable damage to individuals.

136. On reflection, whilst I would suggest keeping this provision under observation to see whether it seems to cause injustice to individuals, I do not conclude that the Act has struck the wrong balance. I do recommend, however, that the Registrar should have a similar power to the court to require the rectification of inaccurate data even if marked as received from a third party. At present the interpretation of the Fifth Principle prevents that. It is difficult to see why inaccurate data should not be amended once it is discovered and the interpretation should be changed so that it does not limit the Registrar's enforcement powers.

(g) The Sixth Principle

137. This Principle restricts the time for which data may be kept to that which is necessary for the purposes for which they are held. There is no interpretation.

138. As in the case of other Principles, there can be difficulty in determining for what purpose data are held. In part (a) of this section I recommended an interpretation to assist in overcoming this difficulty.

139. In addition, as in the case of the Fourth Principle, there is the problem that the time period is related simply to the potentially very broad purpose for which the data are held and takes no account, on the face of it, of the practical effects on data subjects. Again, in part (a) of this section there is a recommendation for an interpretation which should helpfully allow the circumstances of individuals to be taken into account.

(h) The Seventh Principle

140. This Principle requires a data user to give data subjects access to their personal data. The interpretation provisions: confine the Principle to the scope of the substantive subject access provisions in Section 21 of the Act; give some guidance on determining whether a data subject is seeking access at reasonable intervals; and provide that correction or erasure of personal data is appropriate only to ensure compliance with the other Data Protection Principles which are substantive in nature, as opposed to the Seventh which is of a procedural character.

141. I believe this interpretation should remain unchanged, but a later chapter considers Section 21 of the Act and recommends some modification.

(i) The Eighth Principle

142. This Principle requires appropriate security measures to be taken against unauthorised access to, or alteration, disclosure or destruction of personal data and against accidental loss or destruction of personal data. There is guidance on the interpretation of appropriate security in that regard shall be had to physical, logical and personnel security.

143. The consultation document, reflecting a view put to the Registrar, asked whether the Principle should give detailed guidance on security steps to be taken. That view had some support. On the other hand, others believe that this is not practicable and that it is better to rely on a general principle which can be enforced appropriately on its merits in a variety of different circumstances.

144. I take the latter view and I recommend no change to the interpretation of this Principle.

(j) Historical, Statistical or Research Purposes

145. A special interpretation is applied to the First and Sixth Principles where data are subsequently used for historical, statistical or research purposes.

146. I do not recommend any change here. It would be wrong to destroy the historical record, or to prevent access to the raw material which can give us greater understanding by use for statistical or research purposes. There is protection in that these beneficial interpretation provisions are subject to the condition that the personal data are not to be used in such a way that damage or distress is, or is likely to be, caused to any data subject.

(k) General

147. Enforcement action can only be taken against registered persons. The clear majority responding to the consultation believe that all data users, even if exempted from bureaucratic controls such as registration, should comply with the Principles. However, it seems unlikely to be practical to cause data users to comply with the Principles other than through the enforcement provisions of the Act.

148. A further, rather technical point, is that the Principles generally apply to data rather than to the action of individuals. However, enforcement action must necessarily be taken against persons—whether legal or natural; so it is not always clear how a data user or computer bureau can contravene a Principle which, because of its wording and the provisions of Section 2(2) of the Act, applies to data.

149. I recommend that both problems could be solved if Section 2 of the Act were amended to include a clear duty on data users to ensure that all eight Data Protection Principles are satisfied in respect of the personal data held by them and if a similar duty to ensure compliance with the Eighth Principle were imposed on computer bureaux. These duties to be subject to the enforcement provisions of the Act.

B2.3 The Register and Registration

(a) The Consultation

150. The consultation document set out a number of purposes which registration might serve and asked what, if any, registration system should continue for the future. Much of the response to the consultation dealt with registration and proposals varied from minor administrative tidying up to the repeal of any registration requirement. The general tenor of the response was to seek some considerable simplification of the present system, particularly as it affects small users. I have sympathy with this general view.

(b) The Options

151. The options available would seem, broadly speaking, to be:

— retain the present system substantially unchanged;

— repeal any requirement for registration;

— radically simplify registration by requiring universal registration of very limited information;

— restrict registration to users, data or purposes judged to be particulary sensitive;

— adopt a two-tier registration where there might be greater detail required for users, data or purposes judged to be particularly sensitive.

152. I do not conclude that registration is an essential requirement of the Council of Europe Convention. There may be difficulties in the way of providing a data protection system without registration, but the proposal of some respondents that registration should be abolished is not to be dismissed out of hand. To decide the best way to go, a view has to be taken of the different purposes a registration system can serve.

(c) Purposes of Registration

153. The consultation document suggested a number of possible purposes for registration. These are set out below and then each of them is considered in turn:

— registration provides a means by which Article 8(a) of the Council of Europe Convention can be satisfied, in that data subjects can find out from the register who keeps personal data, what the data user's address is and why he keeps the data;

— registration is a public declaration of openness by data users, encouraging understanding of and debate about practices in processing personal data;

— the register gives data subjects an address at which they can apply for subject access with certainty;

— the Registrar can refuse to register any applicant thought not likely to comply with the Principles. Registration therefore offers a possibility for reviewing and determining the acceptability of a data user's activities;

— in the Act, registration is also related to enforcement through the de-registration process. If a data user who should be registered is refused registration or de-registered, then he commits an offence of strict liability if he continues to process personal data;

— the register is a practical aid to enforcement because it gives the Registrar a list of those who should be checked to ensure they are complying with the Act;

— there is a source of revenue to fund data protection enforcement.

154. It has also been suggested that the register can give sufficient notice to those from whom information is obtained to satisfy the "fair obtaining" requirement of the First Data Protection Principle. I am advised that the law would have to deem that everyone had notice of the register if it were to perform that role. Others have asked whether it should be possible for any individual to check from a register who actually holds data about him or her. Leaving aside any issue of law; experience suggests to me that there is no practical way in which a register can satisfy either of these objectives.

155. The first purpose set out above was to satisfy Article 8(a) of the Council of Europe Convention. This provides that any person shall be enabled:

> "a. to establish the existence of an automated personal data file, its main purposes, as well as the identity and habitual residence or principal place of business of the controller of the file".

156. There is no need to register data users to achieve this purpose. It is possible simply to enact legal duties requiring data users to respond to enquiries by providing the information referred to in Article 8(a). That could be said to satisfy the Convention.

157. It is worth bearing in mind at this point, that Article 5(b) of the Convention requires personal data undergoing automatic processing to be "stored for specified ... purposes". That requirement is reflected in the Second Data Protection Principle. The specification of the purpose for which data are stored or held ought to take place no later than the start of the storage or holding in question. It may be difficult to enforce this requirement, if a data user can, undetected, adjust the purposes for which he has been holding data when subjected to an investigation. Registration may assist in overcoming this problem.

158. Registration is a means of concentrating the minds of data users. It requires them to describe their activities in respect of personal data and make open declarations that they are within the scope of data protection legislation and can be expected to comply with its requirements. It is undoubtedly the case that having to register has made many organisations think through their data handling arrangements and has concentrated minds on the issue. Whilst this has undoubtedly assisted the implementation of the Act, it is not of itself a reason for adopting a registration system with the considerable burdens which it might cast on data users. However, if data users do not describe their activities openly, the opportunity if lost for public learning and debate. I return to this point later.

159. Having an address for subject access on the register can be a benefit to a data subject seeking to enforce his legal rights. If he has sent a proper request, by recorded delivery, addressed to the subject access address proferred by the data user, that data user can hardly say the request was not made. It is not essential to have such an arrangement, but it is an undoubted improvement on having to rely on the normal legal rules for the service of documents. However, the value of this is conditioned by the opportunities available for any given individual to examine the register and determine the subject access address.

160. The present registration system gives a power to the Registrar to refuse applications if there is doubt whether a data user will comply with the Princi-

ples. It is doubtful whether, under the present system, resources could realistically be made available to check each applicant in any effective manner. Registration could, in practice, only be used as an effective vetting system, if the numbers required to register were very significantly reduced. Nevertheless, if there are wide exemptions from registration, or the detail to be registered is reduced, then the Registrar's power to protect individuals is lessened. I return to this point later.

161. Currently, registration is linked to enforcement through a de-registration process. This is not essential. It would be quite possible to substitute a data holding prohibiting notice, if registration were dispensed with in whole or in part.

162. A register can provide a list of those with whom contact should be maintained; at whom publicity, advisory and educational material should be directed; and who should be visited to check and promote compliance. The first two objectives are best satisfied with as comprehensive a register as possible, whereas the last objective might only realistically be pursued if the register were confined to a smaller group of those data users who were thought to raise particular data protection concerns.

163. The need to finance the implementation of data protection cannot be overlooked and is a desirable, if not essential, aspect of registration. Universal registration of all data users could lead to a reduction in fee. Selective registration could require significantly increased fees – levied largely on those who give rise to data protection concerns.

(d) The Present System

164. Complaints about the present system arise principally from small data users. They consider their activities to be non-sensitive but find that they are required to comply with what they see as a complex and bureaucratic process. They do not see how their involvement in the process furthers data protection objectives. Their problems have been reduced, but not entirely eliminated by the Short Registration Form (DPR4) which was introduced in the Autumn of 1987.

165. From the data subject's point of view, the register is a great disappointment. It is large and complex and provides only limited help in directing an individual to where information about him or her might be held.

166. The criticisms of the present system are largely correct. It would be wrong not to make some attempt to deal with them and see if there are other ways of achieving the objectives which registration might have been hoped to fulfil. Retaining the present system substantially unchanged does not seem to be a proper long-term objective.

167. On the other hand, there are reasons for not repealing registration entirely. The benefits of a list of those who are data users, who are therefore known to the public and can be addressed by the Registrar, and from whom revenue is raised to finance data protection, are reasons for retaining a form of registration.

(e) Universal Simplified Registration

168. One option to the present method is a system of universal, but simplified registration. With very few exceptions all data users and computer bureaux could be required to register. The payroll and accounts exemption, the mailing list and unincorporated members club exemptions would be repealed. The exemption for private, domestic and recreational use should remain. I assume that public policy would require a continuing exemption for national security matters.

169. Under this system, each data user would register its name and address as at present. In addition, each would give a short description of its main business or organisational activities. There could be an option for data users to add an address for subject access enquiries if the main registered address did not fulfil this purpose. Computer bureaux would register as at present.

170. There would be consequential changes to the criminal offences related to the content of a register entry. The Registrar should be able to refuse an application if he had reason to believe that the proposed register entry details would be inaccurate or misleading.

171. Such a system would include more data users in the scope of the system. It would be radically simplified. There would be no need to specify the details of data subjects, data classes, sources and disclosures, nor attempt to fit activities to standard purposes. It would be more akin to the vehicle or television licence systems. The system would remove doubts about the application of some of the exemptions; it would enable data users and bureaux to declare that they were within the scope of the Act; it would be linked to a de-registration process; it could give a subject access address; it would give a comprehensive contact list for advisory material to be addressed to data users; and it would raise revenue. The fee payable by each person registered should be relatively small.

172. On the other hand, the system would clearly not exclude all those small data users who are burdened by the present system and who, in reality, may be doing little to cause concern to individual members of the public. The system would create a potentially large tail of data users who should register, but who are likely to be reluctant so to do. A significant, and probably unacceptably large, resource would have to be devoted to ensuring that the recalcitrant were investigated and prosecuted. Resources would be diverted from investigating matters of proper data protection concern.

173. Universal registration would provide a large list with whom contact could be maintained by mailing material, but it would be an unrealistically large list to assist in the enforcement of the Act. The number would be too great to maintain any reasonable level of contact seeking to ensure that the Principles were complied with. Similarly, the number would be too great for a proper examination to be made of the merits of each application to register with a view to deciding whether or not to refuse it.

(f) Restricted Registration

174. A number of other countries—for example, West Germany and Ireland—see a benefit in registering certain types of data user, but they avoid universal registration. A decision has to be made about the activities which are likely to be of greater, rather than lesser, data protection concern. If that can be done in practice, then the system can be confined to relatively few data users. Their fees will fund data protection enforcement. The smaller number can more readily be advised and visited by the Registrar.

175. A common approach elsewhere is to say that public sector authorities should always register. To these can be added a list of those handling sensitive data such as identified in the Convention, or engaging in sensitive activities. The problem, and one of the principal disadvantages of restricted registration, is the difficulty in setting boundaries.

176. The present Act seeks to define cases where an exemption applies. It may be simpler, with a restricted registration system, to define who is included rather than who may be excluded. Those to be included might be defined as follows:

1. Government Departments.
2. Those holding personal data for the prevention of detection of crime, or the

apprehension or prosecution of offenders. This would cover Chief Officers of Police and Police Forces and some larger organisations with their own investigative and security units.

3. Other Public bodies including any local authority, statutory undertaker (as conventionally defined), and similar bodies.
4. Persons conducting public examinations and granting educational qualifications.
5. Professional regulatory bodies.
6. Persons concerned in the provision of banking, insurance, investment or other financial services.
7. Persons subject to Part III of the Consumer Credit Act 1974.
8. Persons concerned in the provision of detective, inquiry, tracing or other investigation services.
9. Persons concerned, in the course of trade or business, in obtaining personal data with a view to supplying them to or allowing their use by others. This might include direct marketing and employment vetting services.
10. Persons concerned in the provision of medical, dental, opthalmic or other health services or services ancillary thereto.
11. Persons holding or processing personal data revealing racial origin, political opinions or religious or other beliefs, physical or mental health or sexual life, or criminal convictions. Except that registration would not be required where the person holding or processing such data gives to each data subject, at least once a year, such information relating to the data as would have to be provided in response to a subject access request. Thus, those who hold health information for employment purposes could exempt themselves from registration in respect of this simply by keeping their employees informed.
12. Those persons who transfer personal data outside the United Kingdom.

177. To that list might be attached a power for the Secretary of State to add, by order, categories of those who should register.

178. Under this arrangement, the important element is that those organisations of data protection significance can be identified by the Registrar and by data subjects. The most important information to be registered therefore is the name and address of the data user and perhaps an address for subject access. The register would be more meaningful if it also contained a short description of the activities of the registered organisation and stated the reason why it had to register. In brief, there seems no compelling reason why greater detail should be registered than under the simplified universal system discussed earlier.

179. The list of those having to register presupposes a decision about what matters or organisations are likely to give rise to data protection issues. The list above is based on the experience of other countries; the provisions of the Council of Europe Convention; my understanding of the views of the public gained from research; and the complaints brought to me by individuals.

180. I have considered the suggestion in the consultation document that those who hold data with the express and informed consent of data subjects should be exempt from registration. I am persuaded by the representations of those who say that this would raise complex issues about whether consent was real and informed and I do not therefore recommend an exemption framed in that way.

181. There is clearly considerable scope for debate about the list of those who should register. Each of the categories mentioned is likely to need further

definition. In particular, it may be appropriate to consider exemptions for published information which might be caught under category 9. I am concerned that the categories in the list should be readily definable and applicable in practice; but even so, complex drafting seems unavoidable in drawing up the definitions. It would not be helpful if data users had to go to immense effort to decide whether or not they had to register.

182. If a list such as that set out above could be agreed upon, then the necessarily limited resources of the Registrar could be devoted to those data users thought to be of special data protection interest. Of course, complaints about breaches of Principles by non-registered data users would also have to be investigated. The organisations of significance would pay for the administration of data protection. The small routine user could escape bureaucratic control, whilst still having to comply with the Data Protection Principles and hence proper data protection practice. Complete exemptions from the Act are dealt with later, but would apply in the same cases as for universal registration.

183. A preliminary analysis of the existing Register suggests that there would be about 50,000 register entries under a restricted system such as that described. To raise the same amount of revenue, the current fee would have to increase at least threefold. A fee of perhaps £200 for a three year registration might seem unduly burdensome on small organisations and individuals and there could be a number of these. It is possible therefore that a scale of fees would have to be established and criteria identified for marking the steps on the scale. Measures might include such as turnover or number of employees. Determining a sensible and easily applicable charging system would not be easy. A study would be required to develop a suitable scheme.

184. A restricted registration system would require further consequential changes to the Act. A Data Holding and Processing Prohibition Notice would be required to regulate non-registered data users who persistently or outrageously breached the Principles. The criminal offence provisions would have to be amended to take account of the limited information registered.

(g) Two-tier Registration

185. There are advantages in having a large revenue base and a comprehensive list of data users to communicate with. Those advantages point to universal registration. On the other hand, there are equally compelling reasons for concentrating effort on and securing payment from those data users identified as of particular significance.

186. There might be a two-tier route which combines the universal and restricted registration schemes. Under such a scheme, some would register in greater detail than others, perhaps akin to the current registration requirements. Those who are required to register in greater detail might also be required to pay a higher fee.

187. I am not convinced that there is any significant advantage in a two-tier system and believe that universal or restricted systems of registration offer better options.

(h) Preferred Option

188. The problems are reasonably clear. The solution is not so clear cut. The advantages and disadvantages of the options have been discussed earlier. The simplicity and ease of definition of universal simplified registration is very attractive. This might well be the easiest scheme to understand and implement. I attach considerable weight, however, to the strong feeling, commonly expressed, that small routine commercial enterprises are not undertaking

activities of major data protection significance. They ought to comply with the Data Protection Principles, but if at all possible, be relieved of the bureaucratic burden of registration.

189. On the other hand there will be great problems in agreeing and defining a restricted list of those who should register and in constructing scales of fees. Investigating and identifying those who should register may be as complex as investigating and pursuing the large numbers of small data users who should register under the universal system.

190. I would welcome a debate on the system to be adopted, but on balance, in order to remove those who are not of data protection significance from the registration net, I favour the restricted registration option and the rest of my recommendations are made with that option in mind.

191. Remodelling registration on the restricted lines described would have further consequences. For those not entirely exempt from the Act, there is the need to satisfy the requirements of Articles 5(b) and 8(a) of the Council of Europe Convention (see part (c) of this section). Even if it were possible to do this, by registration for those who must register, the problem would still remain for those who need not register.

192. To meet these Convention requirements I therefore recommend that all data users should be under a duty to maintain an up to date list of the purposes for which they hold or use personal data. Also, on request from any person, they should inform that person of those purposes and, in general terms, of the personal data held or used in connection therewith. I would expect to use my power to give advice under Section 36(3) of the Act to publish recommended purpose descriptions which I hope data users would find helpful. Whilst not specifically concerned with registration, it may also be possible to draw up descriptions of the sort of data and types of disclosures which might normally be associated with those purposes.

193. Many fewer particulars would be registered. Consequently, the provisions of Section 4(3), 5(1), 5(2) and 5(3) of the Act will require major modification. Those sections of the Act specify what must be currently registered and make it a criminal offence not to register, or to do something not allowed for in a register entry whether it is done by the data user, his servant or agent. The consequence would be a much restricted application of the criminal law. On the other hand, a criminal sanction would be required to secure compliance with the new duty to keep a list of purposes and provide it to enquirers.

194. The rules relating to fees are probably sufficiently flexible to allow scales of fees to be modified without further legislative change. In the light of the very limited particulars proposed to be registered, it might be valuable to declare that the Registrar can require further information from applicants for registration in order to determine whether to exercise his power of refusal. The suggestion for a power to issue an Information Notice is discussed again in the next chapter.

195. Finally, it should be remembered that registration, as currently conceived in the Act, requires data users to be open, at least in general terms, as to their activities in respect of personal data. If registration is to be restricted, as recommended, then this openness through registration is lost. In addition, the restricted detail which will be registered under the system put forward removes any possibility of the Registrar checking, from registration applications, whether data users may be acting, or likely to act, in breach of the Data Protection Principles. In the light of these two points, there needs to be some compensating adjustment elsewhere in the Act — perhaps in the rights of individuals to know and the powers of the Registrar to find out. I seek to retain an appropriate balance in the recommendations put forward later.

B2.4 Supervision and Enforcement

196. The Act is enforced chiefly by the Registrar. He can prosecute for some matters—not being registered and straying outside the scope of a register entry, for example. Breaches of the Data Protection Principles are dealt with by Enforcement, De-registration and Transfer Prohibition Notices. Failure to comply with a confirmed notice is a criminal offence. There are various ancillary provisions such as the power to seek a warrant.

197. The consultation document canvassed some possible changes. The proposal to give the direct right of enforcement to individuals is discussed in the next chapter. The matters to be considered here include the limited right of the Registrar to obtain information in an investigation and related technical problems in the warrant procedure; the role of the Tribunal; defects in the supervisory notice powers; and the question of inspection by the Registrar.

198. The Registrar, in the course of investigating breaches or suspected breaches of the Principles, often requires information from a variety of sources. The ability to obtain it in a formal and evidentially authoritative manner would be valuable. My investigators have reported that individuals working for organisations often feel hesitant about giving evidence because they cannot be assured that they are under a duty to do so. Those individuals would be happier to co-operate, as seems to be their natural inclination, if they could be told that the Registrar could exercise formal powers to require them to answer questions. In the section on registration, I have already mentioned the need to obtain adequate information on the basis of which a decision can be taken to refuse registration. I recommend, as a solution to these difficulties, that the Registrar should have power to serve notice on any person requiring that person to furnish in writing such information (as specified in the notice) as is necessary or expedient for the performance by the Registrar of his functions. There should be a right of appeal against such a notice to the Tribunal.

199. The Registrar has no express investigation powers. Investigations are carried out because they are essential if proper consideration is to be given to those complaints which the Registrar has a duty to consider. Also, because no proper decision on prosecution or the exercise of supervisory powers can be made without the systematic gathering of evidence. Currently, my officers can only seize evidence with the backing of a warrant. A warrant may only be granted if access is refused and subject to strict conditions. Consequently, if access is granted, an investigator is deprived of the right to apply for a warrant and thus cannot seize evidence. I recommend that the arrangements should be clarified by granting, to duly authorised officers of the Registrar, the power to seize evidence when lawfully on premises whether under a warrant or not.

200. The opportunity could be taken to amend a further weakness in the warrant procedure. The powers of inspection and seizure do not apply to data which are exempt from Part II of the Act (which deals with registration and supervision). My recommendation for restricted registration would require a change to that reference to Part II, but in any case the protection from inspection and seizure poses logical and practical difficulties. It is only after they have been looked at that it is possible to tell whether or not the data are exempt. In the cases where warrants have been obtained, it has been necessary to take magnetic media away from premises for subsequent technical examination. Only at that stage is it clear whether the protection from seizure applies. Data may already have been seized which should have been protected. The warrant powers therefore become hazardous. To avoid this, I recommend that the protection of data from inspection and seizure should be repealed.

201. The consultation document asked whether all data protection matters should be referred to the Tribunal. Some respondents emphasised that points of law should be settled by the ordinary courts. That does not mean that other matters should not be considered at a lower level by the Tribunal. The Tribunal has, at the time of writing, yet to sit. Similarly, I am not aware of any case brought by an individual to the ordinary courts seeking to recover compensation under the Act. I am, therefore, conscious that it might be premature to comment, but I would recommend that all cases should be heard initially by the Tribunal so that the Tribunal can develop a broad data protection perspective. The Tribunal would replace the ordinary courts for hearing applications by individuals to enforce their subject access rights or to claim compensation. Appeals on points of law would lie to the higher courts. The issue of the right of individuals to apply to the Tribunal for the direct enforcement of the Principles is considered in the next section.

202. If the changes recommended for the registration system are adopted and if all data users holding personal data are bound to comply with the Data Protection Principles irrespective of registration, then the format and content of the powers relating to Supervisory Notices must be changed. Firstly, it should be possible to serve a notice on any data user holding personal data and any computer bureau processing personal data rather than, as at present, serving notices on registered persons. Secondly, de-registration loses its effectiveness if the majority of those bound to comply with the Principles do not have to register. Registration should no longer be linked to enforcement in this way, and for the De-registration Notice I recommend that there should be substituted a Data Holding and Processing Prohibition Notice which could include the de-registration of any data user registered under the proposed restricted system.

203. Irrespective of any change to the registration system there is a difficulty with the Transfer Prohibition Notice. The Transfer Prohibition Notice provisions refer to prohibiting the transfer of "data". Data means "information recorded in a form ..." In R v Gold & Another [1988] 2 WLR 984 (HL), the House of Lords held that data held in the registers of a central processing unit could be said to be recorded, which was a word contemplating more permanent retention and, in the case of data, implied the use of something such as tape or disc recording. Commonly, computerised information is transferred outside the United Kingdom not by sending physical objects such as magnetic tape on which data are recorded, but by transmitting data by a telecommunications link. In those cases, what is transferred is not actually recorded, but a replica of the recorded data.

204. In any dispute, I would point out that the decision in R v Gold was a decision on the meaning of "recorded" in the Forgery and Counterfeiting Act, 1981 and does not necessarily apply to the term "recorded" in the Data Protection Act in relation to overseas transfer. Nevertheless a Transfer Prohibition Notice might be held by the courts not to protect personal data recorded in the United Kingdom from abuse outside the United Kingdom. I recommend that Section 12 of the Act should be amended to put beyond doubt the fact that the transfer of data, by transmitting a copy of the data by radio, cable or similar technical means, can be regulated by a Transfer Prohibition Notice.

205. During the last four years my office has sometimes met great difficulty in deciding which of two or more persons is a data user and therefore responsible for securing compliance with the Principles for a particular set of personal data. Those who have been involved in discussions about pension fund trustees and administrators; accountants and their clients; and some computer bureaux activities will recall the difficult distinctions that had to be made. The problem chiefly arises where a lay client goes to a professional adviser. The professional adviser may apply automated techniques to personal data on which only the adviser is competent to judge and where sometimes the lay client may even be ignorant that a computer is being used. The problem would cease to be of such

significance if the Registrar could take enforcement action not only against the data user but also against a person by whose default a data user was in breach of the Data Protection Principle. I recommend that such a power should be applied to all the Supervisory Notices.

206. An issue canvassed in the consultation document was whether the Registrar should carry out systematic inspections of data users. Perhaps not surprisingly, the majority of respondents rejected the suggestion on the ground that it would be an unnecessary intrusion into the affairs of data users when there was no significant evidence of regular data abuse.

207. However, as mentioned earlier, a simplified registration system would remove a possibility of public scrutiny on, or debate of, data users' activities and limit the ability of the Registrar to check those activities. Information would generally only be brought to light in specific cases of complaint. In these circumstances, I believe it is appropriate to compensate for this shift in balance and some power of inspection by the Registrar would seem an appropriate part of that. I therefore recommend that such a power should be added to the Act.

208. There is one special point which arises from the concern expressed by correspondents about disclosures of information. I accept that it would be too onerous as a general rule for data users to keep logs of sources and disclosures. However, it does seem right, when information is found to be inaccurate, for every effort to be made to inform others supplying or receiving it of this fact. I therefore recommend an addition to Section 10(3) of the Act which refers to an Enforcement Notice in respect of inaccurate data. The addition should specifically allow the notice to require a data user to take all reasonable steps to inform any source of information and those to whom it has been disclosed of the inaccuracies found.

209. Finally, a number of respondents suggested that government departments should not be excluded from liability to prosecution. I understand those views. I also understand, however, that such an exclusion is long standing matter of public policy. I therefore leave this issue for consideration if future experience shows that particular difficulties arise from it. An amended Act could include an order-making capacity which would allow the status of government departments to be changed if this seemed to be necessary.

B2.5 Rights of Data Subjects

(a) Role of the Tribunal

210. Data subjects do not currently have the right to enforce the Act directly except to secure subject access and to obtain compensation, or in certain limited cases to get rectification or erasure of personal data. It would be possible to give individuals the right to seek compensation either from the courts or the Tribunal for any breach of the Data Protection Principles causing damage to that individual. Others have canvassed the possibility of compensation for distress irrespective of damage. Undoubtedly, breaches of privacy can cause types of damage not accounted for in traditional legal notions of damage and I would welcome a debate about whether distress alone should justify compensation.

211. Other variations have been proposed on the idea that individuals should be able to enforce the Act directly. One proposal is that an individual should have a right of appeal to the Data Protection Tribunal against the refusal of the Registrar to take formal action against a data user.

212. I have sympathy with this idea but it is difficult to put into practice because of the respective roles of the Tribunal, the Registrar and the data user. The Tribunal is not an investigative body, it judges a case which is made by the Registrar against a data user. If the Registrar would not pursue such a case, then an individual appealing to the Tribunal would have to take the Registrar's role; the individual could not simply ask the Tribunal to overturn the Registrar's view. In the case in which an individual believed that the Registrar's actions were not properly taken in accordance with his powers, then the remedy is in judicial review through the Courts. But judicial review would not apply to the merits of a decision.

213. I conclude that currently, while a data user can appeal to the Tribunal against a supervisory notice, there is no corresponding way for a data subject to object to a failure by the Registrar to take enforcement action. Pursuing the idea of a balance between the rights of data users and data subjects I would recommend therefore, that data subjects should be given the power to seek from the Tribunal an order which would have the same effect as a confirmed Enforcement Notice or other Supervisory Notice. The Tribunal ought to be given the opportunity to stay such proceedings so that the Registrar can investigate such cases before they are heard by the Tribunal. The Registrar could then be a party to the proceedings; he would not necessarily be supporting the application for an order.

214. For an individual a breach of a Principle may be incapable of remedy. Steps can be taken to ensure there is no repetition of the breach in a future case, but the only satisfaction to the hurt individual in such a case is compensation. I recommend, therefore, that the Registrar should be given the right to include, in a Supervisory Notice, a direction to pay compensation to an individual for damage and associated distress arising from a breach of Principle. The compensation should be limited to a sum not exceeding the financial limit on claims in the County Court—currently £5,000. The Registrar is currently under the supervision of the Council on Tribunals and the exercise of discretion in recommending compensation seems not inappropriate to an official in this quasi-judicial position.

(b) Subject Access

215. The most significant right of individuals is the right of subject access. A number of questions about this were put in the consultation document and a substantial number of responses were received. These are summarised in Chapter 1.

216. With a restricted registration system, I believe there should be counter balancing changes in the information an individual can obtain from a data user. I have referred in Section B2.3 to the need for a duty for data users to maintain an up to date list of purposes and to give copies of this to enquirers. However, with the loss of detail in the Register, individuals have lost any possibility, other than through a subject access request, of linking data held about them to particular purposes, sources or disclosures.

217. I recommend, therefore, that in response to a subject access request, a data user should provide not only the data about the individual, but also a description of the purposes for which the data are held or used. These descriptions of purposes might be simply achieved by cross references to the list of purposes mentioned above.

218. I would also recommend that a description should be given, at least in general terms, of the disclosures which may be made of the data. This might be simply achieved by limiting these descriptions to disclosures not covered by a non-disclosure exemption. It would also be helpful if some indication could be given of the sources of the data. I am very mindful of the problems in connection with providing information on sources and disclosures. These ideas would certainly need thinking through very carefully but, if they could be put into practice, they should help to meet a number of concerns expressed by respondents to the consultation.

219. Then there is the question of the fee for subject access. The issue of multiple fees being charged for multiple register entries would disappear under a restricted registration system, because many data users would have no register entry and the remainder would have only one entry. The size of the fee itself is still a matter of debate. Research suggests that the public favours a fee lower than £10 and may be deterred from exercising the subject access rights by a fee this high. It would therefore be helpful to reconsider the fee with that in mind. I would recommend that, at least, the fee should be held at no more than its present level for some time. In addition, steps should be taken to set a limit on the total amount an individual can be charged for access to multiple register entries, if these continue to exist.

220. Next is the difficulty of dealing with the situation where information is withheld from an individual under a subject access exemption. The individual does not know that the data user has applied an exemption and is in no position to make an appeal to test whether the exemption has been properly applied or not. Although a number of respondents deny that there is a problem, the statute plainly sees circumstances in which granting subject access would prejudice the purpose for which data are kept, or cause other serious harm. It seems highly likely that there will be cases where to tell a data subject that data has been withheld for those reasons would cause the same damage contemplated by the statute. It might well be that those respondents who say that this is a smaller class of cases than is often supposed are right, but a solution to the dilemma is required.

221. I recommend that data users should be required to keep a log of the cases in which a subject exemption is relied upon and the reasons for using the exemption. The log should be available for inspection by the Registrar or his officers. I recommend that data users should be required to make a periodic return to the Registrar, sending him a copy of the log. That duty would have to be reinforced by a criminal penalty.

222. I note the difference of opinion about the meaning of Section 21(4)(b) of the Act. This section allows a data user to refuse subject access if the information disclosed would also relate to another individual, or would identify another individual as the source of the information. This section has not, however, been the subject of litigation, and it may be premature to propose changes here until the practical effect of the legislation can be more clearly seen. If the Sub-section is reviewed then consideration should be given to the right of the enquiring individual to know the information; the right of the other individual to privacy; and the right of a data user to protect his sources of information.

223. The consultation document asked whether individuals should have the right to know that data are held about them by a particular data user without having to make a subject access request and without having to pay a fee. There was a difference of opinion between respondents about this suggestion. But it must cost as much in most cases to find out whether data are held about a particular individual as to provide a copy of that data. I would not recommend a right to have the former free, if a fee remains chargeable for the latter.

224. Many are enthusiastic about data users keeping source and disclosure logs. If this were practicable, some problems relating to enforcement could more readily be solved—for example, contacting people to whom inaccurate data has been transmitted, or determining a source to resolve an issue of fair obtaining. In the light of the views of respondents, I am persuaded that such logs might be inordinately expensive, and in some cases quite impractical—library catalogues are an extreme but realistic example. I cannot, therefore, support a universal requirement for source and disclosure logs. However, I do note that some such logs are kept at present by credit reference agencies. I believe further consideration should be given as to whether there are other special circumstances in which such logs should be kept.

B2.6 The Exemptions

225. There should be an enforceable duty for all within the scope of the Act to comply with the Principles; but the duty to register should be greatly restricted. With this approach the exemptions can be narrowed and simplified and many of the current problems with exemptions should disappear.

226. I recommend complete exemption from the Act for data held by an individual only for personal, domestic or recreational purposes. I assume that public policy will continue to require an exemption on the current lines for national security.

227. I recommend a modification to the current exemption for data which the data user is required by statute to publish. I would make that a non-disclosure exemption. It is difficult to see why the data user should be released from all the Principles, for example that relating to accuracy, merely because he has to publish the information. I return later to the issue as to whether there should also be a subject access exemption for this data.

228. The exemption for payroll and accounts (Section 32 of the Act), and mailing lists and unincorporated members clubs (Section 33(2)) would no longer be required in the light of the revised scheme for registration and the duty to comply with the Principles recommended earlier.

229. The remaining exemptions in Part IV of the Act are either from subject access or from the non-disclosure provisions. There has been some debate about the extent of these exemptions.

230. I do not recommend any changes to the limited subject access exemptions for crime, taxation, health, social work and financial services provided they are properly confined to cases where there is a real likelihood of the problem specified by the Act arising in each case. I hope that the recommendation that the use of the subject access exemptions should be logged and reported to the Registrar will make it possible to monitor their use.

231. I do not take issue with the non-disclosure exemptions in subsections 5 to 8 of Section 34 of the Act. They seem to cover cases of legal compulsion, emergency or common sense. In the case of new legislation, it may be that policy makers will increasingly consider data protection objectives and whether it is always right to be able to rely on the exemptions in the Data Protection Act for things done under statutory authority. There have been positive responses when I have approached Ministers and their departments with this in mind. At this stage I would only recommend a modification to these limited exemptions in order to take account of the repeal of the non-disclosure provision contained in Section 5(2)(d) of the Act. This limits disclosures to those stated in a register entry and under a restricted registration scheme, this detail would no longer be provided.

232. Many respondents have suggested that the definition of personal data should be framed so as to exclude bibliographic information or names associated with products, services or business contact lists. I later conclude that it is not appropriate to try to redefine personal data so as to draw a boundary between information about individuals and information about organisations.

However, I do have sympathy with the general objective behind respondents' suggestions. It seems to me that if the personal data outlined fall outside registration then the only difficulty remaining is that of subject access. There seems no reason why the information described should not meet the other Data Protection Principles, for example, it should be fairly obtained. Exemptions from the subject access right should be strictly limited and very carefully defined. I do not feel able to define a specific recommendation at present, but I believe it would be worth exploring possibilities. A study to do this might also consider whether a subject access exemption might apply to other, strictly defined, published information.

B2.7 The Registrar's Powers

233. Revised enforcement powers for the Registrar were proposed earlier, but the consultation document raised a number of further points.

234. I have undertaken this review of the legislation to assist the Home Office and as part of my general duty to report to Parliament on the performance of my functions. Most of those who have commented express the view that this is a helpful practice. A few believe that this is a matter of policy for politicians alone. It seems to me that, as in the case of the Equal Opportunities Commission and the Local Government Commissioners, it ought to be helpful to policy makers and legislators to have the views of the enforcing authority on the impact of legislation of this nature. It is also consistent with the expectation that public bodies should monitor and report on their experience in carrying out their functions. It would be valuable to put the practice which I have adopted on an express statutory footing.

235. The idea that the Registrar should have the power to support court applications by individuals received some backing. The Act has regard to the balance of policy between the rights of people to keep, use and pass on information, and on the other hand, the rights of individuals to have respect shown for their privacy. However, the general tenor of the legislation is to create rights and duties which place a fetter on the otherwise unrestricted rights of the users of information. In that context, it would be helpful in enforcing those rights and duties, on occasion, for the Registrar to support an individual conducting his own proceedings under the Act. I recommend that an extra power to that effect should be added to the Act.

236. The remaining major issue in this section is the role of codes of practice. Some suggest that detailed statutory codes should be prepared for each sector and that compliance with such codes should replace compliance with the Data Protection Principles.

237. I have come to disagree with that view. The great effort required to define sectors and develop precise codes in fine detail would, in my view, divert resources from encouraging compliance with the powerful and flexible Principles. The Principles give a broad basis on which the Tribunal and courts can build. They are flexible enough to take account of sectoral differences, the variation of individual cases and the development of new technologies.

238. On the other hand, there is a role for codes of practice as a guide to compliance with the Principles. I recommend that the Registrar should have power to give a formal endorsement to codes so that they could have a similar force to the Highway Code. Thus, compliance with or breach of a code would be taken into account by the Tribunal, but breach of a code would not of itself amount to a breach of a Principle.

B2.8 General and Miscellaneous

239. Section 39 of the Act deals with data held or services provided outside the United Kingdom. Many, including my office, find Section 39 complex. That is in part unavoidable, because the issues it seeks to resolve are notorious for creating legal difficulty. I earlier suggested a strengthening of the provisions relating to Transborder Data Flows. I recommend a further minor change: the reference in Section 39(5) to data being used in the United Kingdom should be changed to a reference to the use of information constituting the data. Without this change, it is difficult to make any meaning of this section. That done, I would leave the other elements of section 39 to be examined by the courts.

240. I mentioned, in the consultation document, the practice of requiring an individual to exercise his rights of subject access in order to reveal his criminal record. I do not believe this is a proper use of the Act. I recommend that it should be prohibited with a criminal sanction. There are undoubtedly cases in which, when someone seeks employment or a licence, his criminal record should be available. Those cases should be specifically provided for in other legislation and not achieved by what many see as an abuse of the Data Protection Act.

241. The third issue raised under this heading was that of administrative flexibility. Many relatively minor issues have arisen such as the form of registration of partnerships, or the occasional refund of fees, for which it would have been helpful to have express statutory authority. There will always be such minor matters arising and I recommend that there should be an appropriate regulation making power for the Registrar. I should make it clear that this regulation making power should be strictly limited to minor administrative matters such as those mentioned above and regulations should have to be approved by the Home Secretary.

B2.9 Definitions

242. None of the definitions in the Act has been subject of legal argument in the higher courts. It is difficult to argue other than academically that they are defective except in a few clear cases. There were nevertheless some particular issues canvassed in the consultation document.

243. I would myself amend data by deleting the reference to "recorded", but there is opposition on the basis that this would introduce control over transient data to which subject access could not be granted. I do not myself feel the force of this argument. Any data routinely held for less than 40 days can escape subject access under the present law. Deleting the reference would put beyond doubt the applicability of our law to transborder data flows affected other than by sending abroad disk, tape or similar recording media. An alternative approach to the specific problem, however, would be to leave the definition of data unamended and, as recommended earlier, add a suitable sub-section to Section 12 of the Act, which authorises Transfer Prohibition Notices. A suitable addition would declare that transmissions of data by radio, cable or similar means are to count as transfers of data notwithstanding the fact that no recording medium containing the data is transferred overseas. For the moment, I would be content with this less thoroughgoing alternative.

244. The consultation document raised the possibility that there might be information which ought properly to be said to relate to an organisation rather than an individual. The difficult exercise of drawing the boundary between these types of data will probably not be helped by amending the definition of "personal data" at this stage. In my view, this is another matter for the courts, in the light of whose decisions future amendments of the Act might arise. I have dealt under the exemptions (Section B2.6) with such particular issues as bibliographic data.

245. The distinction between "opinion" and "intention" breaks down. The distinction was introduced to protect personnel succession planning data from subject access. The provision is far wider than is necessary for the intended purpose: it has the effect of exempting this and other data from the whole Act when a subject access exemption for this particular data would have been sufficient. If what is required is the right to maintain the confidentiality of personnel succession planning data, then I recommend that a specific narrow exemption to that effect should replace the present distinction between "intention" and "opinion".

246. It is difficult to give a precise meaning to the text processing exclusion. However, the general intent seems clear enough. It has not been argued about in the higher courts. Surprisingly, it seems to work in practice. I would leave well alone and do not recommend any amendment.

247. The definition of "data user" in Section 1(5) of the Act is complex. I recommend deletion of the words "form part of a collection of data" in paragraph (a) and the substitution of the word "are". In paragraph (b) I recommend deleting the words "jointly or in common". In the first case, it is not clear what counts as a collection of data, because first of all one must identify a single data item. Whether that is a complex "piece of information" or something else is so doubtful as to cause grave difficulty of interpretation. In the second case, it is quite clear that the Act means to include as a data user

someone who controls data by cooperating in some way with another person. The technical words "jointly or in common" are confusing and best omitted.

248. The use of "agent", both in the definition of computer bureau and also in the expression "servant or agent" elsewhere, needs refining. In the Act "agent" seems usually to mean someone authorised to create legal relations between a principal and a third party, rather than someone acting generally for another. The courts might resolve the problem, but this is a case in which either approach to the meaning of "agent" can lead to answers which are difficult to accept. Generally speaking I believe "agent" in the Act should bear the broad meaning of an intermediary through whom someone effects an action and, for the avoidance of doubt, recommend the word should be thus defined.

249. I recognise that some respondents to the consultation document take a distinctly different view from me about what is meant by processing "by reference to the data subject". A narrow interpretation excludes matters which commonsense would often suggest should be included—for example, searching for people who have a common characteristic such as religion or ethnic origin. I do not agree that this form of processing lies outside the Act. I recommend amending the definition by expressly including processing by reference to classes of individuals.

250. "Processing" does not currently fully include some matters which are within the Council of Europe Convention. It is consequently not clear how the Act exactly corresponds to the Convention. For the avoidance of doubt and unnecessary legal argument, I recommend including "storage" and "transmission" of data within the definition of "processing".

251. Finally, I raise an issue for further consideration. The broad terms of the Act are sufficient to include electronic office systems including the filing of electronic correspondence where it can be retrieved by reference to the data subject. The Council of Europe have indicated that the application of data protection subject access provisions to such data might amount to a breach of Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedom which guarantees to everyone respect for his correspondence. It might be possible to adjust the definitions in the Act to remove such correspondence from the scope of the legislation. That might create unacceptable data protection loopholes encouraging people to put data artificially into "correspondence". I suggest that more consideration should be given to this problem. It might be appropriate to resolve it by a limited subject access exemption for correspondence, having in mind that which would properly fall under the Human Rights Convention.

B2.10 Overview

252. This overview describes the nature and summarises the main effects of the recommendations made in this chapter. It does not state all of the recommendations specifically or in detail. The main paragraph references are given to assist a reader who wishes to consider the recommendations more closely.

(a) The Data Protection Principles

253. There should be an enforceable duty on data users, with very few exemptions and regardless of whether they are registered or not, to comply with all eight Data Protection Principles. Computer bureaux, as now, should have an enforceable duty to comply with the Eighth Principle. (Paragraphs 147–149)

254. The Principles themselves should remain unchanged but there should be a number of changes to the interpretation provisions. Given the restricted registration system recommended later, there will in any case need to be changes to the interpretation provisions of Principles 2 and 3 which refer to the Register. (Paragraphs 103–105, 126–128)

255. Some new interpretations are recommended to help in the application of the general rules the Principles lay down. These interpretations:

— link the purposes for which personal data are held to the purposes for which they were obtained; (Paragraphs 106–108)

— relate the circumstances of data subjects to consideration (under Principles 4 and 6) of whether personal data are adequate, relevant, not excessive, or kept for longer than necessary; (Paragraphs 109, 110)

— give guidance on fair obtaining (Principle 1) in circumstances where the personal data obtained are to be supplied to or made available to others for their own uses; (Paragraphs 113–115)

— relate unfair processing (Principle 1) to the purposes of the processing and the foreseeable consequences for data subjects; (Paragraphs 120, 121)

— link the specification of a purpose (Principle 2) to a form approved by the Registrar and to the circumstances in which and purposes for which the personal data were obtained; (Paragraphs 124, 125)

— bring into consideration, when determining whether a disclosure is incompatible with the purposes for which personal data are held (Principle 3), the purposes for which the data are to be used by the person to whom they are disclosed. (Paragraph 130)

256. Other recommended changes to current interpretations act so as to:

— Open the possibility of applying the fair obtaining requirement (Principle 1) to information which is statutorily required, in circumstances where this is unlikely to prejudice the statutory purpose for which the information is required. This should even up the application of the Act between the public and private sectors; (Paragraphs 116–119)

— allow the Registrar to take normal enforcement action in respect of inaccurate data which a data user has received from others and marked as so received (Principle 5). The present interpretation prevents this but it does seem

in everybody's best interests to take corrective action on inaccurate data once it is discovered. (Paragraphs 134–136)

(b) The Register and Registration

257. Whether the Act is changed in the near future or not, it is not sound long term policy to continue with the current registration system. However, it is sensible to continue with a registration system of some form. The arguments supporting this conclusion and the following recommendations are contained in section B2.3.

258. The two best options appear to be a universal registration system which might be compared to obtaining a TV license; or a restricted registration system where only defined categories of data users need to register. In both these cases it would be appropriate to register only a limited amount of information. Bearing in mind the problems for small, non-sensitive data users, the second option is preferred. A successful scheme will, however, depend on how clearly those categories of data users who must register can be defined. More work is required on these definitions. Consideration will also need to be given as to whether there should be a graduated scale of fees for those who must register.

259. It is recommended, therefore, that registration should be maintained, but on a restricted basis. Rather than determining the restrictions through exemptions there should be a list of those who should register. A list is put forward for discussion in section B2.3. It is based on type of organisation, type of activity and those holding sensitive personal data. There should be an order making capacity for the Home Secretary to add to the list. First estimates suggest that the Register would reduce to about one third of its present size and contain around 50,000 registrations. This would lead to a fee of around £200 for a three year registration.

260. The detail to be registered should comprise only a name and address, an optional address for subject access, a brief indication of the nature of the organisation registering and the registration category under which the entry is made.

261. In order to meet the requirements of the Council of Europe Convention there should be a duty on data users to maintain a list of the purposes for which they hold personal data together with a broad indication of the types of data kept for each purpose. The duty should include supplying a copy of this list to any enquirer on demand. This new duty should be reinforced with a criminal sanction similar to that for failing to register. (Paragraphs 191–193)

262. Restricting registration will remove an opportunity for the public to know about data users' activities . It will also remove an opportunity for the Registrar to consider the practices of applicants for registration. There should be compensating changes in the rights of individuals and the powers of the Registrar.

(c) Supervision and Enforcement

263. With a restricted registration system the offences for undertaking activities not in accordance with the current detailed register entries will disappear. The Act will need amending to take account of this. It will still be an offence not to be registered, but this will not of course apply to data users who are not required to register.

264. The Registrar should have power to serve a Supervisory Notice on any data user holding personal data or computer bureau processing personal data whether or not they are registered. (Paragraph 202)

265. The Registrar should have power to serve an Information Notice on any person requiring that person to furnish in writing such information specified in the notice as may be necessary or expedient for the performance by the Registrar of his functions. There should be a right of appeal against such a notice to the Tribunal. (Paragraph 198)

266. Duly authorised officers of the Registrar should have the power to seize evidence when lawfully on premises whether under a warrant or not. (Paragraph 199)

267. The protection of any data from seizure under a warrant should be repealed. The present provisions make data seizure a hazardous or impractical matter. (Paragraph 200)

268. All data protection claims by individuals should be heard in the first instance by the Data Protection Tribunal with an appeal on points of law to the higher courts. (Paragraph 201)

269. A Data Holding and Processing Prohibition Notice should replace the current De-registration Notice. This will bring registered and non-registered users onto a par with each other. As far as those who are registered are concerned the new notice could incorporate a de-registration provision. (Paragraph 202)

270. The Registrar should be able to serve a Transfer Prohibition Notice where the transfer abroad is by radio, cable or similar technical means and not by physical transfer of a recording medium. (Paragraphs 203, 204)

271. The Registrar should have power to serve supervisory notices not only on a data user but also on any person by whose default a data user is in breach of a Data Protection Principle. This would assist small, unsophisticated data users whose processing is undertaken by professional service providers. (Paragraph 205)

272. The Registrar should be empowered to inspect the activities of data users. This would counterbalance opportunities lost by the change to a restricted registration system. (Paragraphs 206, 207)

273. The Registrar should be able, when issuing an Enforcement Notice in connection with inaccurate personal data, to require a data user to take all reasonable steps to inform any source of the data and those to whom the data have been disclosed, of the inaccuracies found. (Paragraph 208)

(d) Rights of Data Subjects

274. I have sympathy with the view that data subjects should be able to appeal to the Tribunal against decisions of the Registrar. However, as explained in Section B2.5 this is not really feasible. In these circumstances to obtain balance with data users, who do have access to the Tribunal, data subjects should have the right to seek from the Tribunal an order which would have the same effect as a confirmed Enforcement Notice or other Supervisory Notice. The Registrar should have the opportunity to investigate such cases and appear as a party before the Tribunal. (Paragraphs 211–213)

275. The Registrar should have the power to include in a Supervisory Notice a direction to pay limited compensation to a data subject for damage and associated distress arising from a breach of a Data Protective Principle. This would cover cases where it is impossible to remedy the breach in question, although it might be possible to prevent it occurring again. (Paragraph 214)

276. There should be some form of balancing right to make up for the loss of information arising from adopting a restricted form of register. In response to a

subject access request, a data user should provide an individual with a copy of his data and a description of the purposes for which it is held or used. (Paragraphs 216, 217)

277. At the least, the fee for subject access should be held at no more than its present level for some time. The problem of individuals having to pay multiple fees, where users have more than one register entry, would disappear under the registration system proposed. (Paragraph 219)

278. In addition, in response to a subject access request, information should be given, perhaps in restricted or general terms, to the sources or disclosures related to the data. The feasibility of this recommendation needs further, careful, consideration. (Paragraph 218)

279. Data users should be required to maintain logs of the cases in which they rely on subject access exemptions and the reasons for so acting. Periodic returns should be made to the Registrar. The log should be open to inspection by the Registrar. These duties should be reinforced by a criminal penalty. (Paragraph 221)

(e) The Exemptions

280. The current exemptions can be narrowed and simplified, particularly as the burden of registration for small data users should largely disappear with a restricted registration system.

281. There should be complete exemption from the Act for data held by an individual only for personal, domestic or recreational purposes. I assume that public policy will require an exemption on the current lines for national security. The exemptions for payroll and accounts, mailing list and unincorporated members clubs should be repealed. (Paragraphs 226, 228)

282. The current extensive exemption for information held by a data user which he is under a statutory duty to publish should be reduced to a non-disclosure exemption. (Paragraphs 227)

283. The definition of the non-disclosure provisions should take account of the repeal of Section 5(2)(d) which is concerned with registered disclosure. The restricted registration system will not require this level of detail. (Paragraph 231)

284. There should be a careful assessment of the possibility of a subject access exemption for personal data connected with bibliographies, product or service descriptions, contact lists for use within and between organisations and information made public by statute. (Paragraph 232)

(f) The Registrar's Powers

285. Revised enforcement powers have already been dealt with. Three further issues are covered here.

286. The Registrar should have an express duty to keep the Act under review and to report on possible modifications. (Paragraph 234)

287. It would be helpful in enforcing the rights and duties under the Act if, on occasion, the Registrar supported an individual conducting his own proceedings under the Act. There should be a power to do this. (Paragraph 235)

288. I do not believe that it is practical to set meaningful, flexible and detailed codes of practice and enshrine these in statutory form. However, codes of practice can give helpful guidance, in particular circumstances, as to how to

meet the requirements of the Data Protection Principles. To encourage their establishment and use, the Registrar should have the power to give formal approval to them. Compliance with approved codes, or a breach of them, would be taken into account by the Tribunal in any proceedings, but breach of a code would not of itself amount to a breach of a Principle. (Paragraphs 236–238)

(g) General and Miscellaneous

289. There should be a minor change to Section 39 of the Act which deals with data held or services provided outside the United Kingdom. This should be amended to so that the reference to data being used in the United Kingdom refers to the use of information constituting the data. (Paragraph 239)

290. I do not believe that requiring an individual (perhaps a job applicant) to exercise his subject access rights in order to reveal a criminal record is a proper use of the Act. Those cases where this is a requirement of public policy should be clearly provided for in other legislation. To prevent this abuse of the Data Protection Act, it should be a criminal offence to compel another to exercise his rights of subject access in order to gain information which would not otherwise be obtainable. (Paragraph 240)

291. There have been occasions, for example, in order to refund fees, when some flexibility in administering the Act would have been helpful. To cope with such requirements, the Registrar should have strictly limited power to achieve minor administrative flexibility by regulations to be approved by the Home Secretary. (Paragraph 241)

(h) Definitions

292. None of the definitions in the Act have been the subject of legal argument in the higher courts. I would therefore leave them substantially untouched.

293. I understand how helpful it might be to have some definitions of personal data which set some boundary between this and information which might more properly be called "organisational" data. I can think of no helpful suggestions at this stage and would again leave the matter to the courts. (Paragraph 244)

294. However, I do believe the exclusion of intentions from the definition of "personal data" should be repealed. I understand that the objective of the exclusion was to protect personnel succession planning data from the data subject. If this is still considered appropriate, a limited subject access exemption to that effect should be substituted. (Paragraph 245)

295. The definition of data user could be improved by removing the requirement to hold "a collection of data" and by repealing the words "jointly or in common". (Paragraph 247)

296. The word "agent" is used in the Act and it is not clear what meaning should be given to it. It should be defined as someone by whom another effects an action. (Paragraph 248)

297. There are conflicting views about what is meant by "processing by reference to the data subject". To avoid doubt and unnecessary legal argument, the definition should expressly include processing by reference to classes of individuals. (Paragraph 249)

298. To line up with the Council of Europe Convention, "storage" and "transmission" of data should be added to the definition of "processing". (Paragraph 250)

299. Finally, a limited subject access exemption for correspondence should be considered to avoid any conflict between the Act and Article 8 of the European Human Rights Convention. (Paragraph 251)

E. J. Howe
Data Protection Registrar
June 1989

Appendix BA1

What Are Your Views?—Twelve Important Questions

1. Should there be a duty on all data users to comply with the Data Protection Principles?
2. Which, if any, of the interpretation provisions of the Principles in Part II of Schedule 1 to the Act should be repealed or amended?
3. Can the register usefully be simplified? Should it contain less detail?
4. Can the need to register be removed from certain classes of data user and computer bureau? If so, how would the exemptions be defined and justified?
5. What should be the enforcement powers of the Registrar? Should he carry out systematic inspections of data users? Should he be able to demand information?
6. Should powers be given to individuals to enforce the Act by applying direct to the Data Protection Tribunal?
7. If information is withheld from an individual on the grounds of a subject access exemption (eg. because giving the information is likely to prejudice the prevention or detection of crime), should the individual be told the exemption has been applied? What if that might itself prejudice the reason for the exemption?
8. What is the right policy on subject access fees?
9. Should codes of practice be legally enforceable or have some other status such as that of the Highway Code? Should there be a duty on trade sectors to prepare codes of practice?
10. Is it objectionable for an organisation to make an individual use his subject access rights in order that the organisation may see his police record? If so, should this be made a criminal offence?
11. Is it possible to define "personal data" more clearly by, for example, excluding information relating to businesses or which is in the "public domain"? Should "data" have to be recorded?
12. Is there any other point about the definitions on which you would wish to comment, e.g. the distinction between "opinion" and "intention" and the "text processing" exclusion?

Appendix BA2

Background to the Data Protection Act

Why a Data Protection Act?

Computers are in use throughout society—collecting, storing, processing and distributing information. Much of that information is about people (personal data). The Data Protection Act 1984 gives new rights to individuals about whom information is recorded on computer (data subjects). They may find out information about themselves, challenge it, have it corrected or erased if appropriate, and claim compensation in certain circumstances. To help members of the public use these rights the Registrar has an important ombudsman role.

The Act places obligations on those who record and use personal data (data users). They must be open about that use (through the Data Protection Register) and follow sound and proper practices (the Data Protection Principles). The Act should raise public confidence in computing and improve practice among computer users. It has also allowed the United Kingdom to ratify the Council of Europe Convention on Data Protection. If the United Kingdom could not ratify the convention it could damage our international trade and some companies might decide to move their operations—and jobs—elsewhere.

What the Act Covers

The Act only applies to automatically processed information—broadly speaking, information which is processed by a computer. It does not cover information which is held and processed manually—for example, in ordinary paper files. Not all computerised information is covered by the Act, only that which relates to living individuals. So, for example, it does not cover information which relates only to a company or organisation.

The Data Protection Principles

Registered data users must comply with the Data Protection Principles in relation to the personal data they hold. Broadly they state that personal data shall be:

— collected and processed fairly and lawfully;

— held only for lawful purposes described in the register entry;

— used only for those purposes and only be disclosed to those people described in the register entry;

— adequate, relevant and not excessive in relation to the purpose for which they are held;

— accurate and, where necessary, kept up to date;

— held no longer than is necessary for the registered purpose;

— protected by proper security.

The Principles also provide for individuals to have access to data held about themselves and, where appropriate, to have the data corrected or deleted.

Registration

Anyone who holds personal information about living individuals on computer should register unless they are covered by one of the very limited

exemptions provided by the Act. People or organisations who have personal data processed by a bureau, or perhaps by their accountant, are still "data users" even if they do not have their own computer.

Apart from the name and address of the data user, the information which has to be supplied for inclusion in the register is a description of the purpose for which it is used, the type of information held, where it is obtained, to whom it will be disclosed and a list of any countries outside the United Kingdom to which it may be transferred. Registration costs £56 for a three year period. Application is made on forms DPR1 or DPR4 (for smaller users). On both, Part A requires details about the user and Part B requires details about the data held. Computer bureaux—in broad terms that means anyone processing personal data on someone else's behalf—also need to register. To register as a bureau only the name and address need be supplied and the £56 fee paid.

Enforcing the Act

The Registrar ensures that the Data Protection Principles are observed. He can serve an Enforcement Notice directing a registered person to take specific steps to comply. He can issue a De-registration Notice cancelling from the register the whole or part of any register entry, thus stopping the user from processing personal data. The Registrar can also issue a Transfer Prohibition Notice to prevent the transfer of personal data overseas. Someone receiving one of these notices can appeal to the independent Data Protection Tribunal. The Tribunal has the power to substitute its own decision in place of the Registrar's.

If the Registrar considers that a criminal offence has been committed under the Act, he may prosecute the offender in the criminal courts and a fine may be imposed. In Scotland the Procurator Fiscal will bring any prosecutions. To obtain evidence of a criminal offence or a breach of principle the Registrar may apply for a search warrant to enter and search any premises.

Individual Rights

Since 11 November 1987 any individual has been entitled to be supplied by a data user with a copy of any personal data held about him or her. This is called the "subject access" right. Individuals write direct to the user for their data, or they may consult the register to obtain more details about the user. Each entry on the register shows the name and address of the data user, a description of the type of information held, how it is gathered and used, and to whom it will be disclosed. It also shows an address where subject access requests may be sent.

Data users may charge up to £10 for meeting each request but some may decide to charge less, or nothing at all. They have up to 40 days in which to provide the data from the date of receiving adequate information to help them locate the data or identify the individual making the request. If the data are not provided within the 40 days, the individual concerned can complain to the Registrar or apply to the courts for an order that the data user should provide access.

A person who has suffered damage and any associated distress caused by the loss, unauthorised destruction or unauthorised disclosure of information about themselves, or through that information being inaccurate, can seek compensation through the courts. If personal data are inaccurate the individual may complain to the Registrar or apply to the courts for correction or deletion of the inaccurate information.

Anyone who considers there has been a breach of one of the Principles, or any other provision of the Act, is entitled to complain to the Data Protection Registrar. When the Registrar has considered the complaint he must notify the complainant of any action which he proposes to take.

Who is exempt?

There are a number of exemptions under the Act. Where personal data are exempt from the whole of the Act those data need not be registered, there is no right of subject access and the Registrar and courts have no powers regarding those personal data. Some exemptions are unconditional, for example where national security is involved, or where an individual holds personal data for recreational purposes or for managing his own personal, fami'y or household affairs. Other exemptions have very strict conditions which m st be complied with before the data can be deemed exempt; for example, whe : data are held for payroll, pensions and accounts, they are exempt unless they are also used for, say, personnel records or marketing purposes, which they are in the majority of cases. Other conditional exemptions exist for unincorporated members' clubs and mailing lists. In the case of all the conditional exemptions the data may not be disclosed, for example, to an outside maintenance engineer without the consent of the individual to whom the data relate. Limited disclosures are permitted for the payroll, pensions and accounts exemption without the consent of the individual.

There are also a number of exemptions from the need to provide information under the subject access provisions of the Act. Some examples of where personal information may be withheld are where this would prejudice:

— the prevention or detection of crime;

— the apprehension or prosecution of offenders;

— the assessment or collection of any tax or duty.

Decisions to withhold information under these exemptions can be challenged by the Registrar on receipt of a complaint from a member of the public. There are also other exemptions from subject access which are detailed in the Registrar's Guideline 6 "The Exemptions", available free from his office.

Appendix BA3

The Data Protection Principles

The Data Protection Principles and their interpretation are set out in Schedule 1 of the Data Protection Act 1984 which is reproduced below.

Schedule 1

The Data Protection Principles

Part I—The Principles

Personal data held by data users

1. The information to be contained in personal data shall be obtained and personal data shall be processed, fairly and lawfully.
2. Personal data shall be held only for one or more specified and lawful purposes.
3. Personal data held for any purpose or purposes shall not be used or disclosed in any manner incompatible with that purpose or those purposes.
4. Personal data held for any purpose or purposes shall be adequate, relevant and not excessive in relation to that purpose or those purposes.
5. Personal data shall be accurate and, where necessary, kept up to date.
6. Personal data held for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
7. An individual shall be entitled —
   (a) at reasonable intervals and without undue delay or expense —
      (i) to be informed by any data user whether he holds personal data of which that individual is the subject; and
      (ii) to access to any such data held by a data user; and
   (b) where appropriate, to have such data corrected or erased.

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

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

Part II—Interpretation

The first principle

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

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

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

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

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

The second principle

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

The third principle

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

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

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

The fifth principle

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

The seventh principle

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

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

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

The eighth principle

6. Regard shall be had —

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

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

Use for historical, statistical or research purposes

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

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

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

Appendix BA4

Glossary of Terms

Personal Data consists of information about a living individual, including expressions of opinion about him or her, but excluding any indication of the intentions of the data user in respect of that individual.

A Data Subject is an individual to whom personal data relate.

Data User is an organisation or individual who controls the contents and use of a collection of personal data processed, or intended to be processed, automatically.

A Computer Bureau is an organisation or individual who processes personal data for data users, or allows data users to process personal data on his equipment. An organisation or individual may thus be a Computer Bureau (eg by providing back-up facilities for another data user) without actually being in business as a Computer Bureau as such.

Supervisory Notices are the Enforcement Notices, De-registration Notices and Transfer Prohibition Notices described in sections 10, 11 and 12 of the Act.

The Council of Europe Convention is the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data which was prepared by the Council of Europe and which was opened for signature on 28 January 1981.

Appendix BA5

List of those who responded to the consultation exercise

Advertising Association
N Ainsworth, County Council Data Protection Coordinator
Association of British Insurers
Association of British Travel Agents
Association of Corporate Trustees
Association of County Councils
Association of District Councils
Association of Independent Businesses
Association of Information Management
Association of Mail Order Publishers
Association of Metropolitan Authorities
Association of Pension Lawyers
Paul R. Beckett
British Bankers Association
British Broadcasting Corporation
British Computer Society
British Computer Society (Auditing by Computer Specialist Group)
British Direct Marketing Association
British Library
British Retailers Association
Building Societies Association
Business Equipment and Information Technology Association
Campaign for Freedom of Information
CCN Systems Ltd
CCS Information Protection and Management Consultants
Chartered Association of Certified Accountants
Chartered Institute of Management Accountants
Chartered Institute of Public Financial Accountants
Churches Main Committee
City of Portsmouth
Clerical Medical Investment Group
Harry Cohen MP
A. D. Cole
Commercial Union Assurance Co PLC
Committee of Directors of Polytechnics
Committee of Vice-Chancellors and Principals of Universities of the United Kingdom
Computing Services Association
Confederation of British Industry
Consumers Association
Consumer Credit Trade Association
Convention of Scottish Local Authorities
Department of Health and Social Services (Northern Ireland)
Drapers Chamber of Trade
Engineering Employers Federation
Ewbank Preece (Finance Company)
Faculty of Advocates
A. Fielding
Fife Regional Council
Finance Houses Association

Friends Provident
J. Gilligan
Goodger Auden (Solicitors)
D. W. Hall (Other Profession/Representative Bodies)
Health and Social Services Board — Northern
Health and Social Services Board — Southern
Daniel Heany
IBM
Imperial Cancer Research Fund
Institute of Chartered Accountants in England and Wales
Institute of Chartered Accountants of Scotland
Institute of Chartered Secretaries and Administrators
Institute of Credit Management Ltd
Institute of Data Processing Management
Institute of Personnel Management
John Lewis Partnership PLC
Josiah Wedgwood and Son Ltd
Anthony Korn (Higher Education)
Lambeth Borough Council
Law Society of Scotland
Leeds Permanent Building Society
Library Association
I. Lloyd
G. C. Lloyd-Davis (Other Profession/Representative Bodies)
Linklaters and Paines (Solicitors)
Local Authorities Management and Computer Services
London Borough Association
Martin Hunt (Computing Industry)
Mercedes-Benz (United Kingdom) Ltd
Alan Moss
National Association of Citizens Advice Bureaux
National Association of Pension Funds Ltd
National Chamber of Trade
National Computing Centre
National Computer Users Forum
National Consumer Council
National Council for Civil Liberties
National Federation of Consumer Groups
Nationalised Industries Data Protection Working Party
Newspaper Society
North East Thames Regional Health Authority
Northern Ireland Civil Service
NHS Centre for Information Technology
OFTEL
Parliamentary Committee Cooperative Union Ltd
Irvine Patnick, OBE, MP
F. J. Peters
Polytechnic of Central London
Property Services Agency
Scottish Association of Citizens Advice Bureaux
Scottish Health Service
Sheffield City Polytechnic
Smith and Johnson (Keighley) Ltd
Society of Pension Consultants
South Eastern Electricity Board
South of Scotland Electricity Board
South Western Electricity Board
Standard Life Assurance
J. A. Sterling (Solicitor)
J. V. Timothy (Solicitor)
Touche Ross (Chartered Accountants)
Trade Union Congress

Transnational Data Report
University of Bath
University of Cambridge
University of Dundee
Wessex Regional Health Authority
West Sussex County Council
J. Whitaker and Son Ltd
Wokingham District Council

N.B. We have also received 30 responses from individuals and organisations who wish to remain anonymous.

Appendix BA6

Tables showing some Key Responses

The following tables show some key responses to questions put in the Consultation Document "What are your views".

Table 1 Consultation Document Response
Q.1 Should there be a duty on all data users to comply with the Data Protection Principles?

Class	Yes	No	Unclear	Total Q.1	Responses To Whole Document
Individual	6	0	0	6	13
Consumer Representative Bodies	3	0	0	3	7
Government Department or other Central Government	2	0	1	3	6
Health Authority	1	0	0	1	5
Health Authority Representative Bodies	2	0	0	2	2
Local Government	5	0	0	5	11
Local Government Representative Bodies	5	0	0	5	7
Police Force	1	0	0	1	1
Police Force Representative Bodies	0	1	0	1	2
Other Public Body	0	0	0	0	1
Other Public Body Representative Bodies	1	0	0	1	1
Solicitor or Barrister	5	0	0	5	7
Solicitor or Barrister Representative Bodies	0	0	0	0	3
Accountant	1	0	0	1	2
Accountant Representative Bodies	5	0	0	5	5
Other Profession	2	0	0	2	2
Other Profession Representative Bodies	1	0	1	2	3
Finance Companies & Firms	4	0	0	4	8
Finance Companies & Firms Representative Bodies	5	1	0	6	10
Public Utilities	3	0	0	3	5
Public Utilities Representative Bodies	2	0	0	2	2
Other Trading Companies & Firms	3	0	0	3	8
Other Trading Companies & Firms Representative Bodies	6	0	0	6	10
Churches Representative Bodies	0	0	0	0	1
Charities, including Schools	0	0	0	0	1
Association Clubs & Other Voluntary Bodies	0	0	0	0	1
Association Clubs & Other Voluntary Bodies Representative Bodies	1	0	0	1	3
Higher Education	5	0	0	5	5
Higher Education Representative Bodies	2	0	0	2	2
Computing Industry	2	0	0	2	3
Computing Industry Representative Bodies	6	0	1	7	7
Marketing Organisations	0	0	0	0	2
Marketing Organisations Representative Bodies	0	1	0	1	3
	79	3	3	85	149

Table 2 Consultation Document Response
Q.3A Can the register usefully be simplified?

Class	Yes	No	Unclear	Total Q.3A	Responses To Whole Document
Individual	5	1	0	6	13
Consumer Representative Bodies	3	0	1	4	7
Government Department or other Central Government	3	0	0	3	6
Health Authority	3	0	0	3	5
Health Authority Representative Bodies	1	1	0	2	2
Local Government	3	0	2	5	11
Local Government Representative Bodies	6	0	0	6	7
Police Force	1	0	0	1	1
Police Force Representative Bodies	1	0	0	1	2
Other Public Body	1	0	0	1	1
Other Public Body Representative Bodies	1	0	0	1	1
Solicitor or Barrister	6	0	0	6	7
Solicitor or Barrister Representative Bodies	2	0	0	2	3
Accountant	0	1	0	1	2
Accountant Representative Bodies	4	0	1	5	5
Other Profession	1	1	0	2	2
Other Profession Representative Bodies	2	0	0	2	3
Finance Companies & Firms	3	1	0	4	8
Finance Companies & Firms Representative Bodies	6	1	0	7	10
Public Utilities	3	1	0	4	5
Public Utilities Representative Bodies	2	0	0	2	2
Other Trading Companies & Firms	6	0	0	6	8
Other Trading Companies & Firms Representative Bodies	4	2	0	6	10
Churches Representative Bodies	0	0	0	0	1
Charities, including Schools	1	0	0	1	1
Association Clubs & Other Voluntary Bodies	0	1	0	1	1
Association Clubs & Other Voluntary Bodies Representative Bodies	0	0	0	0	3
Higher Education	5	0	0	5	5
Higher Education Representative Bodies	2	0	0	2	2
Computing Industry	2	0	0	2	3
Computing Industry Representative Bodies	7	0	0	7	7
Marketing Organisations	1	0	0	1	2
Marketing Organisations Representative Bodies	0	0	1	1	3
	85	10	5	100	149

Table 3 Consultation Document Response
Q.4A Can the need to register be removed from certain classes of data user and computer bureau?

Class	Yes	No	Unclear	Total Q.4A	Responses To Whole Document
Individual	4	2	1	7	13
Consumer Representative Bodies	3	1	0	4	7
Government Department or other Central Government	4	0	0	4	6
Health Authority	2	1	0	3	5
Health Authority Representative Bodies	1	0	0	1	2
Local Government	3	3	0	6	11
Local Government Representative Bodies	3	2	1	6	7
Police Force	0	1	0	1	1
Police Force Representative Bodies	1	0	0	1	2
Other Public Body	1	0	0	1	1
Other Public Body Representative Bodies	1	0	0	1	1
Solicitor or Barrister	3	2	1	6	7
Solicitor or Barrister Representative Bodies	0	0	0	0	3
Accountant	1	0	0	1	2
Accountant Representative Bodies	3	2	0	5	5
Other Profession	0	1	0	1	2
Other Profession Representative Bodies	1	1	0	2	3
Finance Companies & Firms	1	4	0	5	8
Finance Companies & Firms Representative Bodies	6	2	0	8	10
Public Utilities	4	0	0	4	5
Public Utilities Representative Bodies	2	0	0	2	2
Other Trading Companies & Firms	2	2	0	4	8
Other Trading Companies & Firms Representative Bodies	7	0	1	8	10
Churches Representative Bodies	1	0	0	1	1
Charities, including Schools	1	0	0	1	1
Association Clubs & Other Voluntary Bodies	0	0	0	0	1
Association Clubs & Other Voluntary Bodies Representative Bodies	1	0	0	1	3
Higher Education	3	2	0	5	5
Higher Education Representative Bodies	1	1	0	2	2
Computing Industry	2	0	0	2	3
Computing Industry Representative Bodies	4	2	0	6	7
Marketing Organisations	1	0	0	1	2
Marketing Organisations Representative Bodies	0	1	0	1	3
	67	30	4	101	149

Table 4 Consultation Document Response
Q.5A Should the Registrar have stronger enforcement powers?

Class	Yes	No	Unclear	Total Q.6	Responses To Whole Document
Individual	4	2	1	7	13
Consumer Representative Bodies	4	0	1	5	7
Government Department or other Central Government	0	0	0	0	6
Health Authority	0	0	0	0	5
Health Authority Representative Bodies	1	0	0	1	2
Local Government	4	0	1	5	11
Local Government Representative Bodies	2	0	0	2	7
Police Force	0	1	0	1	1
Police Force Representative Bodies	0	1	0	1	2
Other Public Body	0	0	0	0	1
Other Public Body Representative Bodies	1	0	0	1	1
Solicitor or Barrister	3	1	0	4	7
Solicitor or Barrister Representative Bodies	0	0	0	0	3
Accountant	0	0	0	0	2
Accountant Representative Bodies	4	0	0	4	5
Other Profession	1	0	0	1	2
Other Profession Representative Bodies	0	3	0	3	3
Finance Companies & Firms	1	2	0	3	8
Finance Companies & Firms Representative Bodies	1	5	0	6	10
Public Utilities	0	1	0	1	5
Public Utilities Representative Bodies	0	2	0	2	2
Other Trading Companies & Firms	1	0	0	1	8
Other Trading Companies & Firms Representative Bodies	0	4	1	5	10
Churches Representative Bodies	0	0	0	0	1
Charities, including Schools	0	1	0	1	1
Association Clubs & Other Voluntary Bodies	0	0	0	0	1
Association Clubs & Other Voluntary Bodies Representative Bodies	1	0	0	1	3
Higher Education	1	2	0	3	5
Higher Education Representative Bodies	1	1	0	2	2
Computing Industry	1	0	0	1	3
Computing Industry Representative Bodies	2	4	0	6	7
Marketing Organisations	0	0	0	0	2
Marketing Organisations Representative Bodies	0	1	0	1	3
	33	31	4	68	149

Table 5 Consultation Document Response
Q.6 Should powers be given to individuals to enforce the Act by applying direct to the Data Protection Tribunal?

Class	Yes	No	Unclear	Total Q.10A	Responses To Whole Document
Individual	5	1	0	6	13
Consumer Representative Bodies	3	0	1	4	7
Government Department or other Central Government	2	0	0	2	6
Health Authority	0	1	0	1	5
Health Authority Representative Bodies	1	1	0	2	2
Local Government	2	0	0	2	11
Local Government Representative Bodies	2	0	0	2	7
Police Force	1	0	0	1	1
Police Force Representative Bodies	1	0	0	1	2
Other Public Body	0	0	0	0	1
Other Public Body Representative Bodies	0	0	0	0	1
Solicitor or Barrister	4	0	0	4	7
Solicitor or Barrister Representative Bodies	0	0	0	0	3
Accountant	0	0	0	0	2
Accountant Representative Bodies	1	1	0	2	5
Other Profession	1	0	0	1	2
Other Profession Representative Bodies	1	1	0	2	3
Finance Companies & Firms	1	1	0	2	8
Finance Companies & Firms Representative Bodies	3	3	1	7	10
Public Utilities	1	0	0	1	5
Public Utilities Representative Bodies	0	2	0	2	2
Other Trading Companies & Firms	0	1	1	2	8
Other Trading Companies & Firms Representative Bodies	2	2	0	4	10
Churches Representative Bodies	0	0	0	0	1
Charities, including Schools	0	0	0	0	1
Association Clubs & Other Voluntary Bodies	0	0	0	0	1
Association Clubs & Other Voluntary Bodies Representative Bodies	1	0	0	1	3
Higher Education	3	0	0	3	5
Higher Education Representative Bodies	1	0	0	1	2
Computing Industry	0	1	0	1	3
Computing Industry Representative Bodies	2	2	1	5	7
Marketing Organisations	0	0	0	0	2
Marketing Organisations Representative Bodies	0	1	0	1	3
	38	18	4	60	149

Table 8 Consultation Document Response
Q.10A Is it objectionable for an organisation to make an individual use his subject access rights in order that the organisation may see his police record?

Class	Yes	No	Unclear	Total Q.12	Responses To Whole Document
Individual	3	0	0	3	13
Consumer Representative Bodies	2	0	1	3	7
Government Department or other Central Government	2	0	0	2	6
Health Authority	1	0	1	2	5
Health Authority Representative Bodies	1	0	1	2	2
Local Government	5	1	0	6	11
Local Government Representative Bodies	2	1	1	4	7
Police Force	1	0	0	1	1
Police Force Representative Bodies	1	0	0	1	2
Other Public Body	0	0	0	0	1
Other Public Body Representative Bodies	1	0	0	1	1
Solicitor or Barrister	2	0	0	2	7
Solicitor or Barrister Representative Bodies	0	0	0	0	3
Accountant	0	0	0	0	2
Accountant Representative Bodies	3	0	0	3	5
Other Profession	1	0	0	1	2
Other Profession Representative Bodies	2	0	0	2	3
Finance Companies & Firms	5	0	0	5	8
Finance Companies & Firms Representative Bodies	3	2	0	5	10
Public Utilities	0	0	0	0	5
Public Utilities Representative Bodies	2	0	0	2	2
Other Trading Companies & Firms	2	0	0	2	8
Other Trading Companies & Firms Representative Bodies	2	1	0	3	10
Churches Representative Bodies	0	0	0	0	1
Charities, including Schools	1	0	0	1	1
Association Clubs & Other Voluntary Bodies	0	0	0	0	1
Association Clubs & Other Voluntary Bodies Representative Bodies	1	0	0	1	3
Higher Education	4	0	0	4	5
Higher Education Representative Bodies	1	0	0	1	2
Computing Industry	1	0	0	1	3
Computing Industry Representative Bodies	5	1	0	6	7
Marketing Organisations	0	0	0	0	2
Marketing Organisations Representative Bodies	0	0	0	0	3
	54	6	4	64	149

Table 7 Consultation Document Response
Q.12 Should a disclosure log be kept?

Class	Yes	No	Unclear	Total Q.5A	Responses To Whole Document
Individual	2	2	0	4	13
Consumer Representative Bodies	2	1	1	4	7
Government Department or other Central Government	0	0	0	0	6
Health Authority	0	3	0	3	5
Health Authority Representative Bodies	1	1	0	2	2
Local Government	1	6	0	7	11
Local Government Representative Bodies	0	2	0	2	7
Police Force	1	0	0	1	1
Police Force Representative Bodies	0	1	0	1	2
Other Public Body	0	0	0	0	1
Other Public Body Representative Bodies	0	1	0	1	1
Solicitor or Barrister	1	1	0	2	7
Solicitor or Barrister Representative Bodies	0	0	0	0	3
Accountant	0	0	0	0	2
Accountant Representative Bodies	1	1	0	2	5
Other Profession	0	0	0	0	2
Other Profession Representative Bodies	0	1	0	1	3
Finance Companies & Firms	0	4	0	4	8
Finance Companies & Firms Representative Bodies	0	6	0	6	10
Public Utilities	0	0	0	0	5
Public Utilities Representative Bodies	0	2	0	2	2
Other Trading Companies & Firms	0	1	0	1	8
Other Trading Companies & Firms Representative Bodies	0	3	0	3	10
Churches Representative Bodies	0	0	0	0	1
Charities, including Schools	1	0	0	1	1
Association Clubs & Other Voluntary Bodies	1	0	0	1	1
Association Clubs & Other Voluntary Bodies Representative Bodies	1	0	0	1	3
Higher Education	1	1	0	2	5
Higher Education Representative Bodies	0	0	0	0	2
Computing Industry	1	1	0	2	3
Computing Industry Representative Bodies	2	3	1	6	7
Marketing Organisations	0	0	0	0	2
Marketing Organisations Representative Bodies	0	1	0	1	3
	16	42	2	60	149

Printed in the United Kingdom for Her Majesty's Stationery Office
Dd 0500759 7/89 C14 58742 3382/1B O/N 65319 5120

The Data Protection Registrar

Springfield House
Water Lane
Wilmslow
Cheshire SK9 5AX