**RESEARCH PAPER 99/99**
3 DECEMBER 1999

# The *Freedom of Information Bill*: Data Protection Issues

## Bill 5 of 1999-2000

This paper complements Research Paper 99/98, *The Freedom of Information Bill*, which describes the main elements of the proposed freedom of information (FOI) regime.

Part I of this paper describes the interface between FOI and the *Data Protection Act 1998*. **Clause 38** of the Bill exempts most "personal data" from the scope of the FOI provisions. Instead, personal data held by public authorities will be available through the *Data Protection Act 1998*, subject to various conditions and exemptions.

Part II of this paper describes the provisions in **Schedule 6** of the Bill which would apply the *Data Protection Act 1998* to Parliament. Part II also provides a brief description of the data protection regime as it applies to Members of Parliament.

Edward Wood

PARLIAMENT AND CONSTITUTION CENTRE

HOUSE OF COMMONS LIBRARY

**Recent Library Research Papers include:**

List of 15 most recent RPs

| | | |
|---|---|---|
| **99/84** | Devolution and Concordats | 19.10.99 |
| **99/85** | The Procedural Consequences of Devolution | 20.10.99 |
| **99/86** | Economic Indicators | 01.11.99 |
| **99/87** | The prospects for Russia | 08.11.99 |
| **99/88** | The *House of Lords Bill* – Lords Amendments [Bill 156 of 1998-99] | 09.11.99 |
| **99/89** | Family Leave | 11.11.99 |
| **99/90** | Unemployment by Constituency – October 1999 | 17.11.99 |
| **99/91** | Millennium Trade Talks – Food and Agriculture Issues | 19.11.99 |
| **99/92** | The *Electronic Communications Bill* [Bill 4 of 1999-2000] | 24.11.99 |
| **99/93** | The Climate Change Levy | 24.11.99 |
| **99/94** | The *Representation of the People Bill* [Bill 2 of 1999-2000] | 25.11.99 |
| **99/95** | By-elections since the 1997 general election | 29.11.99 |
| **99/96** | Economic Indicators | 01.12.99 |
| **99/97** | The *Government Resources and Accounts Bill* [Bill 3 of 1999-2000] | 30.11.99 |
| **99/98** | The *Freedom of Information Bill* [Bill 5 of 1999-2000] | 03.12.99 |

*Research Papers are available as PDF files:*

- *to members of the general public on the Parliamentary web site,*
  *URL:* ***http://www.parliament.uk***
- *within Parliament to users of the Parliamentary Intranet,*
  *URL:* ***http://hcl1.hclibrary.parliament.u****k*

Library Research Papers are compiled for the benefit of Members of Parliament and their personal staff. Authors are available to discuss the contents of these papers with Members and their staff but cannot advise members of the general public.

Users of the printed version of these papers will find a pre-addressed response form at the end of the text.

ISSN 1368-8456

# Summary of main points

Part I describes the arrangements in the current Bill for the interface between the freedom of information (FOI) regime and the *Data Protection Act 1998*. **Clause 38** exempts most "personal data" from the scope of the freedom of information provisions. This does not mean that it will be impossible to obtain documents which contain such data. Instead, personal data held by public authorities will be available through the *Data Protection Act 1998*, subject to various conditions and exemptions.

There are different rules for requests for personal data depending on whether the data relate to the applicant or to a third party (including personal data on officials), and the manner in which the information is held. In practice, it will be easier to obtain information relating to the applicant (known as "subject access") than third parties, but if third party information does not have to be released the public authority will have a duty to consider whether they should make a discretionary disclosure under **Clause 13**. In the case of information relating to the applicant which is held in unstructured paper files, the individual will have to describe what information they wish to see before they may apply to see it.

The Data Protection Registrar, Elizabeth France, has questioned whether the FOI/data protection interface would be "unnecessarily complicated" in practice, particularly if requests for information do not fall neatly into the subject/third party distinction outlined above. She has suggested that very little information falling into the latter category is likely to be disclosed, and has called for a distinction to be made between "personal" information relating to the public and private lives of officials.

Part II of this paper describes the provisions in **Schedule 6** of the Bill which would apply the *Data Protection Act 1998* to Parliament. In addition to applying the Act, a widespread exemption is created where this is necessary "for the purpose of avoiding an infringement of the privileges of either House". A general authority for Parliament to hold personal data, including sensitive personal data, is created, subject to the other duties imposed by the 1998 Act. Part II of the paper also provides a brief description of the data protection regime as it applies to Members of Parliament.

This paper complements Research Paper 99/98, *The Freedom of Information Bill*, which describes the main elements of the proposed FOI regime.

## CONTENTS

# I Data Protection and the *Freedom of Information Bill*

## A. Requests for Personal Data from Public Authorities

The white paper *Your Right to Know* proposed that freedom of information legislation would cover all personal data held by public authorities, whether on computer or on paper files.[1] This would cover a broader range of material than data protection legislation; the two regimes would run in parallel but "we intend to ensure that the regimes for freedom of information and the protection of personal privacy accommodate each other. The two regimes have to perform differing functions as effectively as possible, with the potential for conflict kept to a minimum" (para 4.6). The white paper promised that "as far as practicable we will align the systems for access to personal information under Data Protection and Freedom of Information. This is likely to include the means of access, time limits for reply, charges and appeals" (para 4.11). The new independent Information Commissioner and the Data Protection Registrar would be "required, under the Freedom of Information Act, to consult each other and to exchange information on those cases where both jurisdictions come into play. In the unlikely event of a dispute arising between the Commissioner and Registrar, on which they are unable to reach agreement, this would ultimately be resolved by the Courts" (para 4.13).

The plan for a dual access regime did not appear in the draft *Freedom of Information Bill*, however.[2] Instead it was proposed that there should be a single Commissioner to oversee the data protection and FOI regimes, but the vast majority of requests for access to personal information would be dealt with under the data protection legislation. This proposal is retained for the current version of the Bill as presented in the Commons.

**Clause 16** creates a single office of Information Commissioner to oversee the freedom of information regime and also the *Data Protection Act 1998*.[3]

**Clause 38** exempts most "personal data" (as defined in section 1 of the *Data Protection Act 1998*)[4] from the scope of the freedom of information provisions. This does not mean that it will be impossible to obtain documents which contain such data. Instead, personal data will be available through the 1998 Act, subject to various conditions and exemptions. This approach is consistent with the general approach adopted by the Bill, that information which is "reasonably accessible" to members of the public by means other than FOI should be obtained by that route and is therefore exempt from the FOI legislation (**Clause 19**).

---

1 Cm 3818, December 1997

2 published in *Freedom of Information: Consultation on Draft Legislation*, Cm 4355, May 1999

3 see Research Paper 99/98, p9

4 see p24

Part VII of the *FOI Bill* extends the right of access to personal data under the 1998 Act to all data held by public authorities, including personal information contained in unstructured paper files.[5] Very few other aspects of the data protection regime will apply to this new category of data. In addition to the right of subject access, individuals will have the right, in certain circumstances, to rectify, block, erase or destroy inaccurate data and to obtain compensation for damage and associated distress suffered as a result of inaccurate data or breach of the subject access right.[6]

It is intended that applicants should be able to make a single application for access to information, leaving the public authority in question to decide whether it should be treated as an FOI request, a request for access to personal information under the data protection rules, or both. Although this is a relatively straightforward idea, the provisions which set out the interface arrangements between the *Data Protection Act 1998* and the *Freedom of Information Bill* are somewhat complex. There are different rules for requests for personal data held by public authorities depending on whether the data relate to the applicant or to a third party, and the manner in which the information is held. The account below assumes that a request for information will fall clearly into a single category, but the Data Protection Registrar has suggested that this will not always be the case: more complex requests are considered later.[7]

**i) A subject access request for information held on computer, manual filing systems and medical records, etc**

The simplest aspect of the interface is requests for personal data from the individual to whom the data relates (the "data subject") which are already covered by the *Data Protection Act 1998*. This type of request (known as a "subject access request") will be unaffected by the introduction of FOI. Examples include requests to see personal data held by the public authority on computer, in structured filing systems and in medical, education, social work and housing records. If the information does not have to be provided under the 1998 Act, **Clause 13** of the *Freedom of Information Bill* exempts the public authority from the duty to decide whether to make a discretionary disclosure under the FOI regime. The rules for subject access, which are contained in section 7 of the 1998 Act, include the following features:

---

5 the annex to the explanatory notes to the Bill [Bill 5-EN] contains section 1 of the Data Protection Act 1998 showing the amendments effected by **Clause 67** of the Bill

6 Public authorities holding such data will have to obey the fourth data protection principle, which requires information to be accurate and, where necessary, up to date; and a restricted version of the sixth data protection principle, which requires data to be processed in accordance with the rights of data subjects under the Act. Even these limited provisions will not apply to personnel records which come in this extra category of personal data.

7 The Annex on p31 shows the rules governing access to personal information under the Bill in diagramatic form

Subject to certain exemptions,[8] an individual has the right to be told whether a person or organisation (a "data controller") is holding personal data about them. The individual, or "data subject", is not obliged to give a description of the personal data which they believe may be held. On receipt of a request, it is up to the data controller to establish whether they have any data on that individual. If data is being held, the data subject has the right to be given a description of:

- the personal data;
- the purposes for which they are being processed; and
- those to whom they are or may be disclosed.

The data subject has the right to be given a copy of any data held and any information available as to the source of those data, subject again to the exemptions mentioned above.

Special rules apply where the information held also contains personal data on third parties, including cases where it is necessary to protect the identity of another individual who has provided information.[9] The data controller may not refuse to comply with the request on the grounds of cost, but may charge a small fee. The normal deadline for complying with a subject assess request is forty days, provided all of the information necessary to locate the data has been supplied. If a data subject believes that a data controller has failed in contravention of the Act to comply with a subject access request they may apply to Court for an order forcing the data controller to comply.

Under section 14 of the 1998 Act, a data subject may apply to the Court for an order requiring the data controller to rectify, block, erase or destroy any inaccurate data relating to them.

**ii) A subject access request for "relatively structured information"**

This new category of information is intended to include, for example, "a case file about an individual which contains correspondence about a number of matters relating to that individual and is indexed by reference only to the dates of the correspondence",[10] but not personnel records. The normal rules for subject access contained in section 7 of the 1998 Act, as set out under category (i) above, will apply.

If the information requested does not have to be provided under the 1998 Act, under **Clause 13** of the *Freedom of Information Bill* the public authority is exempt from the duty to decide whether to make a discretionary disclosure.

---

8 relating to a variety of matters including national security, the prevention or detection of crime, etc

9 These rules are described on p15

10 *Freedom of Information Bill: Explanatory Notes*, Bill 5-EN, para 208. There is no formal definition of relatively structured personal data in the Bill: it is that data which is left when "unstructured personal data" (**Clause 68(2)**) is subtracted from the category defined in **Clause 67(2)**.

**iii) A subject access request for "unstructured personal data"**

This category of data, defined in **Clause 68(2)**, is intended to apply, for example, to incidental personal information on individuals which is held in policy files, but not to information which is "structured by reference to individuals" and not personnel records.

Where a request relates to unstructured personal data, the subject access rules are modified as follows. Ordinarily, as explained under category (i) above, an individual is not obliged to give a description of the personal data which he or she believes may be held in order to make a subject access request. In the case of unstructured personal data, however, an individual will have to give a description of the data in question in order to make a subject access request. This might be seen as restricting the usefulness of the subject access rights in relation to this type of information, but given that this kind of information is by definition unstructured, it might be virtually impossible for a public authority to be certain that it had no unstructured personal data on an individual if a catch-all subject access request could be made.

In addition, a public authority will be free to refuse to comply with a subject access request in respect of unstructured personal data if the cost of complying would exceed a limit set by the Secretary of State in regulations. In a case where the cost of complying in full with the request exceeds the specified limit, the data controller will nevertheless be required to inform the data subject whether personal data relating to them are being held if the cost of so doing does not exceed the limit.

If the information requested does not have to be provided under the 1998 Act, under **Clause 13** of the *Freedom of Information Bill* the public authority is exempt from the duty to decide whether to make a discretionary disclosure.

**iv) A request for personal information held on computer, etc, relating to third parties**

This category of information covers personal data which are already covered by the 1998 Act (including data held on computer, in structured filing systems and in medical, education, social work and housing records). Personal data on third parties held by public authorities might include information concerning officials in their official capacity, as well as information on their private lives.

Where access to third party information in this category is requested, under **Clause 38(2)-(4)** the information becomes exempt from the freedom of information disclosure rules if one of three conditions apply:

1. the disclosure would breach one of the 1998 Act data protection principles, whether or not they actually apply to this kind of information;[11]
2. the information falls into one of the categories in part IV of the 1998 Act under which it would be exempt if a subject access request were being made; or
3. the third party has used their right under section 10 of the 1998 Act to require the data controller to stop processing their personal data on the ground that this is causing unwarranted damage or distress.

If some or all of the information does not have to be provided under these rules, **Clause 13** of the *Freedom of Information Bill* requires the public authority to decide whether to make a discretionary disclosure.

**v) A request for unstructured or relatively structured personal information relating to third parties**

This category of information is intended to include loosely structured case files about individuals and incidental personal information on individuals which is held in policy files. It does not include personnel records. Where access to third party information in this category is requested, the information becomes exempt from the freedom of information disclosure rules under **Clause 38(2)-(4)** if one of two conditions apply:

1. the disclosure would breach one of the 1998 Act data protection principles, whether or not they actually apply to this kind of information;[12] or
2. the information falls into one of the categories in part IV of the 1998 Act under which it would be exempt if a subject access request were being made.

If some or all of the information does not have to be provided under these rules, **Clause 13** of the *Freedom of Information Bill* requires the public authority to decide whether to make a discretionary disclosure.

## B. Comments on the Data Protection/FOI Interface

In a memorandum to the Public Administration Committee on the draft Bill, the Data Protection Registrar (DPR) welcomed the proposal to bring to create a single office of Information Commissioner who will have oversight of both the FOI and data protection legislation:[13]

---

[11] Only the fourth data protection principle and part of the sixth data protection principle will apply to this category of personal data. When deciding whether the disclosure would breach a data protection principle, this is to be disregarded and the decision made as if all the data protection principles applied

[12] Only the fourth data protection principle and part of the sixth data protection principle will apply to this category of personal data. When deciding whether the disclosure would breach a data protection principle, this is to be disregarded and the decision made as if all the data protection principles applied

[13] Third Report of 1998-99, *Freedom of Information Draft Bill*, Vol II: HC 570-II of 1998-99, 16.8.99, memorandum 2, p18, para 3

> Both laws relate to aspects of information policy and they come together at the point where personal information is considered for disclosure. […]
>
> The Registrar welcomes the strong role for good practice within the Freedom of Information regime and the way this mirrors the approach in the data protection legislation. The Information Commissioner will be able to provide an integrated, coherent approach to good practice, bringing together the different strands of information handling covered by both regimes. This should benefit public authorities and data controllers.
>
> Another benefit from bringing both regimes under the oversight of one Information Commissioner will be evident where decisions about third party access to personal information require review by the supervisory authority. Such decisions raise data protection and privacy issues. The possibility of institutional conflict which would exist were there to be separate Commissioners for Freedom of Information and data protection matters is avoided.

The DPR agreed that "all access to personal information should involve reference to the 1998 Act" but had "concerns about the complexity of the draft Bill's proposals in practice":[14]

> The draft Bill's general approach seems to be based on the assumption that a request for information will fall clearly into a request for information about the applicant or a request for third party information. This is unlikely always to be the case… A degree of complexity in the interface arrangements between freedom of information and data protection regimes is inevitable. The issue is whether the draft Bill would produce an unnecessarily complicated interface in practice. The Registrar is concerned that any complexity should be kept to the absolute minimum. Access rights should be easy to administer and simple to understand.

In her oral evidence to the Public Administration Committee, the Registrar suggested that even if the complexity of the interface did not present any difficulty for the individual at the point of making a request for information, it might nevertheless make it difficult for them to understand why the request had been refused.[15]

The Public Administration Committee's report on the draft Bill suggested that the relationship between the *Freedom of Information Bill* and the *Data Protection Act* "is achieved in a sensible way",[16] but "its complexity is, however, daunting". The Committee noted the Data Protection Registrar's concerns that these arrangements might

---

14 Ibid, para 4

15 *Minutes of Evidence for Tuesday 22 June 1999*, HC 570-ii of 1998-99, 5.7.99, Q 184

16 Third Report of 1998-99, *Freedom of Information Draft Bill*, HC 570-I of 1998-99, 29.7.99, para 98

prove over-complicated in practice, especially with a more complex request.[17] The Government's response to the Committee's report stated that it will work closely with the Data Protection Registrar to ensure that authorities and applicants have easy to understand guidance.[18]

A description of what the consequences might be if a request for information covered data relating to the applicant and a third party is set out in Appendix II of the DPR's memorandum:[19]

A COMPLEX REQUEST FOR PERSONAL INFORMATION

1. The draft Bill's general approach seems to be based on the assumption that a request for information will fall into one category or the other (ie information about the applicant or third party information). This is unlikely always to be the case. It is possible that requests may involve information about the individual as well as information about third parties.
2. In the case of the former, the information could include:
— information falling within the unamended 1998 Act;
— structured information falling within the additional category to which the section 7 application provisions would apply; and also
— some unstructured information to which the special provisions set out in the new section 9A would apply.
Information about third parties could also be included within the information to be disclosed in the subject access response and that information would be subject to the 1998 Act provisions relating to third party information.
3. However if the information requested also included information relating to third parties which was not linked to the information relating to the applicant, the third party access provisions set out in the draft Freedom of Information Bill would come into play. This third party information could also require a split approach, if a section 10 order were to apply to some of it. For the remainder of the information the other two tests would have to be applied (breach of a data protection principle or whether a subject access exemption would apply).
4. A further complication would be if some of the information requested proved to be exempt from disclosure under the Data Protection Act 1998 subject access provisions (in the case of information relating to the data subject) or under the draft Freedom of Information Bill (in the case of information relating to a third party). The request in respect of that exempt information would then require further consideration under the Freedom of Information regime; a discretionary disclosure would have to be considered.

---

17 Ibid, para 95

18 *Government Response to the Third Report from the Select Committee on Public Administration (Session 1998-99) on the Freedom of Information Draft Bill*, Fifth Special Report, HC 831 of 1998-99, 27.10.99, Appendix

19 HC 570-II of 1998-99, Op cit, Appendix II, p 23

The above example addresses the draft Bill rather than the current version of the Bill. It should be noted that the scope of the discretionary disclosure scheme under **Clause 13** of the Bill is narrower than its equivalent in the draft Bill.[20] Accordingly, if information requested under categories (i)-(iii) in section A above does not have to be provided under the 1998 Act, there is no duty under **Clause 13** to decide whether to make a discretionary disclosure.

The Data Protection Registrar observes that although the rules for third party information (see categories (iv) and (v) in section A above) are an appropriate basis for deciding whether to disclose such data, they "are likely to proved complicated to operate in practice". She suggests that very little information falling under these categories is likely to be disclosed, and notes that the Bill makes no distinction between information concerning the "public" and "private" lives of officials:[21]

> It is the Registrar's view that in practice very little information is likely to be disclosable under these provisions. For example, in the case of sensitive personal data, the disclosable information might be restricted to information where explicit consent for the disclosure has been obtained or information is already in the public domain. It is right that personal information should be properly protected. It is a matter for Ministers and Parliament whether very limited disclosure of personal information to third parties is consistent with the objective of Freedom of Information.
>
> The draft Bill treats all third party requests for access to personal information in the same way. It makes no distinction between what is public and what is private. Yet it would be possible to make this distinction between an official's public activities ie between personal information relating to an official in the course of his duties, and his private life, ie that relating to him as a private individual. Drawing this distinction would permit different approaches towards disclosure of information related to public activities which might be disclosable, or to private life which should usually receive the same protection afforded to individuals not in the public service. This would extend the quantity of personal information potentially available to third parties.

In a note to the Public Administration Committee, the Home Office observed that the DPR's proposal was based on the premise that there is a difference between "public" and "private" personal data:[22]

> This distinction is not set out in the Directive. The terms of the Directive are, to a certain extent, open to interpretation and we believe that it may be possible to develop some guidelines which take account of the Registrar's intentions, but are

---

20 **Clause 14**, Cm 4355

21 HC 570-II of 1998-99, op cit, memorandum 2, p19, paras 4.4-4.5

22 HC 570-I of 1998-99, op cit, Annex 6, note 107

> clearly consistent with the Directive. But we need to discuss this in some depth with the Registrar.
>
> The Directive sets out minimum standards of protection for Data, and it is not possible to provide less protection. As noted above, there is probably room for some interpretation of the Directive (and of the Data Protection Act 1998), but we cannot base legislation on anything other than a firm understanding that what we are doing is consistent with our international legal obligations.

The Government's response to the Committee's report returns to this point:[23]

> The Government has discussed the proposals of the Data Protection Registrar with her. The Government agrees that her proposals are a helpful guide to the interpretation of the EU Data Protection Directive and its interface with the Freedom of Information legislation. The Government understands that the Registrar intends, when she has the powers under the Freedom of Information Act, to refine her proposals and to issue them as interpretative guidance under the provisions of clause 40 of the Bill. The Government welcomes this intention.

The Registrar observes that section 7 of the *Data Protection Act 1998 Act* already provides for cases where a subject access request covers material which also includes personal data about third parties. The DPR's *Introduction to the Data Protection Act 1998* sets out the circumstances where it may be reasonable to provide the information requested, if the consent of the other individual has not been obtained:[24]

> A particular problem arises for data controllers who may find that in complying with a subject access request they will disclose information relating to an individual other than the data subject who can be identified from that information, including the situation where the information enables that other individual to be identified as the source of the information… The Act recognises this problem and sets out only two circumstances in which the data controller is obliged to comply with the subject access request in such circumstances, namely:-
>
> - where the other individual has consented to the disclosure of the information, or
> - where it is reasonable in all the circumstances to comply with the request without the consent of the other individual.
>
> The Act assists in interpreting whether it is reasonable in all the circumstances to comply with the request without the consent of the other individual concerned. In deciding this question regard shall be had, in particular, to:-
>
> - any duty of confidentiality owed to the other individual,

---

23 HC 831 of 1998-99, op cit, Appendix

24 October 1998, p18, chapter 4, para 1.3, also available at www.dataprotection.gov.uk

- any steps taken by the data controller with a view to seeking the consent of the other individual,
- whether the other individual is capable of giving consent, and
- any express refusal of consent by the other individual.

> If a data controller is satisfied that the data subject will not be able to identify the other individual from the information, taking into account any other information which, in the reasonable belief of the data controller, is likely to be in (or to come into) the possession of the data subject, then the data controller must provide the information.

The Data Protection Registrar suggests that it may be possible to use these *Data Protection Act* tests for determining whether disclosure is "reasonable in all the circumstances" as the starting point for assessing requests for disclosure of personal information on third parties under the *Freedom of Information Bill*:[25]

> An extra test, or tests, could be added to cover the cases of disclosure of information about officials acting in their public capacity. This approach would be more economical—it would make use of an existing structure with minimal additions—and would provide a simpler approach than that outlined in the draft Bill.

The Public Administration Committee's report stated:[26]

> We have not sought to give detailed scrutiny to the merits of [the Data Protection Registrar's] proposals. It is certainly not clear to us that it constitutes any clearer a regime than the one in the Bill. **We recommend that the Government respond fully to these proposals in its response to this Report; and that it in any case consider helping those who have to apply these provisions by stating within the Bill itself (rather than indicating through the application of certain provisions of the Data Protection Act) the rules to be applied to requests for third party information. There will undeniably need to be an easy-to-understand guide for authorities on how they should apply these provisions, and we recommend that the Government collaborate with the Data Protection Registrar on the production of such a guide. We believe that applicants should be able to gain access to the information they require without having to establish which Act to use; and that authorities and the Commissioner should work to make this possible.**

---

25 HC 570-II of 1998-99, op cit, memorandum 2, p19, para 4.6

26 HC 570-I of 1998-99, op cit, para 99

# II Data Protection and Parliament

## A. Application of the Data Protection Act to Parliament

### 1. Exclusive Cognisance

**Schedule 6, para 2** of the Bill inserts a new section 63A into the *Data Protection Act 1998* which would have the effect of applying the 1998 Act to Parliament. The "data controller" for the House of Commons would be the Corporate Officer of that House (the Clerk). The data controller for the Lords would be the Corporate Officer of the House of Lords (the Clerk of the Parliaments). Under the new section 63A(4), the data controllers for both Houses would be exempt from prosecution under the Act.

The Joint Committee on Parliamentary Privilege observed recently that the *Data Protection Acts* of 1984 and 1998 Act are taken not to apply within the precincts of either House because there is no express provision in the Act that it should apply. This is an aspect of the doctrine of exclusive cognisance (or exclusive jurisdiction), which is one of the main components of parliamentary privilege. According to this doctrine,[27]

> Parliament must have sole control over all aspects of its own affairs: to determine for itself what the procedures shall be, whether there has been a breach of its procedures and what then should happen. This privilege is […] of fundamental importance. Indeed, acceptance by the executive and the courts of law that Parliament has the right to make its own rules, and has unquestioned authority over the procedures it employs as legislator, is of scarcely less importance than the right to freedom of speech. Both rights are essential elements in parliamentary independence.
>
> Parliament's right to regulate its own affairs includes the **power to discipline its own members** for misconduct and, further, **power to punish anyone**, whether a member or not, for behaviour interfering substantially with the proper conduct of parliamentary business. Such interference is known as contempt of Parliament. This falls within the penal jurisdiction exercised by each House to ensure it can carry out its constitutional functions properly and that its members and officers are not obstructed or impeded, for example by threats or bribes. The sanctions available are reprimand, imprisonment for the remainder of the session and, possibly in the House of Lords, but probably not in the House of Commons, a fine of unlimited amount. Even in the House of Lords the power to impose a fine has not been used in modern times. Members of the House of Commons are also liable to suspension for any period up to the remainder of the Parliament (though there is no modern case of suspension for anything like this length). Members so suspended usually forfeit their salaries for the period of their suspension. Members of the House of Commons can be expelled, although it is over 50 years since the power of expulsion was last used.

---

[27] HC 214-I of 1998-99, paras 13-15

> Another aspect of Parliament's right to regulate its own internal affairs concerns the application of legislation to activities taking place within the Houses of Parliament. In 1934 the courts decided, in the *A P Herbert* case, that the sale of alcohol in the precincts of the House of Commons without a justices' licence was a matter relating to the internal affairs of the House and that no court had power to interfere. Since then, Acts of Parliament have been taken not to apply within the precincts of either House in the absence of express provision that they should apply. Among the legislation taken not to apply are the Health and Safety at Work etc. Act 1974 and the Data Protection Acts 1984 and 1998. In practice Parliament voluntarily abides by some of these statutory provisions.

The Committee recommended that there should be legislation clarifying that in respect of matters not directly and closely related to proceedings in Parliament there should be a principle of statutory interpretation that in the absence of a contrary expression of intention, Acts of Parliament bind both Houses.[28] This legislation should not be retrospective, however, as "a sweeping retrospective change applying to all existing legislation would have unforeseeable practical repercussions". The doctrine of exclusive cognisance does not apply to Members of Parliament in respect of activities which are not "proceedings in Parliament" (their constituency role, for example). Members are therefore bound by the *Data Protection Act 1984* if they hold personal data on individuals in the course of such activities, and will be covered by the *1998 Act* when it comes into force on 1 March 2000 .[29]

The *Data Protection Act 1998* will give effect in UK law to EC Directive 95/46EC (*the Data Protection Directive*). Directives are binding upon Member States but in general they do not have direct effect. In other words, they do not take effect automatically in the legal systems of the Member States; the Member States must give effect to Directives in domestic legislation. There is some discretion as to the method and form of implementation, however. Under the *European Communities Act 1972*, secondary legislation (regulations) may be used to give effect to EU legislation, but in the case of the *Data Protection Directive* the Government considered that it would be better to use primary legislation.

It seems likely that if the *Data Protection Act* is not amended so that it applies to Parliament, the UK Government will be in default of its EU obligations. The question arises as to whether the *Data Protection Directive* might then create some directly enforceable rights for individuals in respect of personal data held by Parliament. In certain circumstances, a directive may create legal effects in the national legal systems of Members States before it has been implemented by domestic legislation. In addition, where an individual has suffered loss as a result of a Member State's failure to implement

---

[28] para 251

[29] see part II(B) of this paper, below

a directive, he or she may be entitled to recover damages from the State.[30] The possibility, in the absence of domestic legislation, of EU legislation creating rights for individuals in respect of actions taken by Parliament would, however, appear to be in direct conflict with the doctrine of exclusive cognisance. This issue has not been tested in the courts and was not considered by the Joint Committee on Privilege. On a strict interpretation of the doctrine of exclusive cognisance, the *European Communities Act 1972* did not expressly bind Parliament, and Parliament is therefore not bound by the Treaties or by legislation made under them. It seems more likely, however, that the courts would set aside the privilege of exclusive cognisance to the extent that it hindered the effective protection of Community law rights.

## 2. Authority to Process Personal Data

The first data protection principle states that personal data[31] must not be processed unless

a) at least one of the conditions in Schedule 2 is met, and
b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

Sensitive personal data includes information as to-

a) the racial or ethnic origin of the data subject,
b) their political opinions,
c) their religious beliefs or other beliefs of a similar nature,
d) whether they are a member of a trade union,
e) their physical or mental health or condition,
f) their sexual life,
g) the commission or alleged commission by them of any offence, or
h) any legal proceedings or sentence for any offence committed or alleged to have been committed by them.

Processing either type of data is permissible if the data subject has given his or her consent.[32] There are a number of alternative conditions under each Schedule. **Schedule 6, paras 3 and 4** of the *Freedom of Information Bill* insert new conditions which permit Parliament to process personal data and sensitive personal data under Schedules 2 and 3 respectively of the 1998 Act. Thus, personal data and sensitive personal data may be processed "for the exercise of any functions of either House of Parliament" (subject, of course, to any of the other requirements of the Act that apply). These provisions are likely to reduce the possibility of any data protection infringements in relation to, for example, constituency cases referred to the Library by Members, but they will not apply to Members in their constituency role.[33]

---

30 Mark Brealey and Mark Hoskins, *Remedies in EC Law*, second edition, 1998, pp 10-11

31 for definition, see p24

32 in the case of sensitive data, *explicit* consent is needed

33 see part II(B) of this paper

## 3. Exemptions for Parliamentary Privilege

Given that the Government intends to apply the 1998 Act to Parliament by means of the FOI Bill, the application of the data protection regime in its current form could have serious implications for parliamentary privilege, particularly parliamentary freedom of speech. However, **Schedule 6** of the Bill contains a number of exemptions in respect of Parliamentary privilege. These are set out in detail later.

The definition of one aspect of privilege, exclusive cognisance, given by the Joint Committee on Parliamentary Privilege was set out above. The Committee summarised the other main aspects of privilege as follows:[34]

> Parliamentary privilege is, in its detail, a complex, technical and somewhat arcane subject. This is partly because of its historic origins and partly because of the multifarious functions of Parliament. Parliament is a legislative and deliberative assembly. Its main constitutional role is to enact the law and, in the case of the House of Commons, to grant supply (that is, make financial provision for the expenses of government). Parliament is also 'the grand inquest of the nation': it is the forum where any grievance may be aired, however small or great. It is the place where the government is called to account by representatives of the whole nation. John Stuart Mill described one task of the legislature as 'to watch and control the government: to throw the light of publicity on its acts'. Ministers can be required to explain to Parliament what is done by them in their capacity as ministers or by their departments, so that members of Parliament can, where necessary, criticise the way public affairs are being administered and public money is being spent. So Parliament must be able to consider any matter it chooses and, principally through its committees, investigate any matter. If there is a national emergency it is only through Parliament that effective action can be taken. The two Houses need sufficient power and authority both to carry out their everyday business and, occasionally, to deal with extraordinary and extreme situations.
>
> **Freedom of speech** is central to Parliament's role. Members must be able to speak and criticise without fear of penalty. This is fundamental to the effective working of Parliament, and is achieved by the primary parliamentary privilege: the absolute protection of 'proceedings in Parliament' guaranteed by **article 9 of the Bill of Rights 1689**. Members are not exposed to any civil or criminal liabilities in respect of what they say or do in the course of proceedings in Parliament. There is no comprehensive definition of the term proceedings in Parliament, although it has often been recommended there should be. Proceedings are broadly interpreted to mean what is said or done in the formal proceedings of either House or the committees of either House, together with conversations, letters and other documentation directly connected with those proceedings.

The *Data Protection Act 1998* places restrictions on the use of personal information by third parties. As suggested above, this could conflict with the privileges of the House, including Members' freedom of speech: their ability, for example, to draft on a computer a speech making allegations about named individuals intended for delivery in the Chamber under the protection of parliamentary privilege. **Schedule 6, para 1** of the current Bill therefore inserts a new section 35A into the 1998 Act exempting Parliament from most of the data protection principles and most of the individual rights available under the Act, *if the exemption is required for the purpose of avoiding an infringement of the privileges of either House of Parliament*. The exemptions given under new section 35A are listed in full below.

The Bill also contains exemptions from the freedom of information regime in respect of parliamentary privilege. Under **Clause 32**, a certificate issued by the Speaker or the Clerk of the Parliaments to the effect that exemption from FOI is required for the purpose of avoiding an infringement of the privileges of their respective Houses "shall be conclusive evidence of that fact". There is no equivalent of the certification procedure under the amended data protection regime as it applies to Parliament.

**Proposed Parliamentary Privilege Exemptions**

1. Personal data are exempt from the following data protection principles under s35A if the exemption is required for the purpose of avoiding an infringement of parliamentary privilege:

- the following part of the first principle: personal data shall be processed fairly and lawfully

- the second principle: personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes

- the third principle: personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed

- the fourth principle: personal data shall be accurate and, where necessary, kept up to date

- the fifth principle: personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes

2. Under s35A the following rights granted to individuals under the *Data Protection Act 1998* **do not apply** if the exemption is required for the purpose of avoiding an infringement of the privileges of either House of Parliament:

---

[34] HC 214-I of 1998-99, paras 13-15

- section 7: right of access to personal data

- section 10: right to prevent processing likely to cause damage or distress

- section 14(1) to (3): right to apply to the Court for an order requiring rectification, blocking, erasure and destruction of inaccurate data

3. **No exemption is granted** from the following data protection principles in respect of parliamentary privilege:

- the following part of the first principle: [personal data] shall not be processed unless-
  a) at least one of the conditions in Schedule 2 is met, and
  b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.[35]

- the sixth principle: personal data shall be processed in accordance with the rights of data subjects under this Act[36]

- the seventh principle: appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data

- the eighth principle: personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data

The exemption for parliamentary privilege is only likely to apply to Members in respect of their participation in proceedings in Parliament: the application of the *Data Protection Act 1998* to Members is considered further in the next section.

## B. Data Protection and Members of Parliament

### 1. Application of the Data Protection Acts

As explained above, under the doctrine of exclusive cognisance the *Data Protection Acts* of 1984 and 1998 do not bind Parliament since they do not specifically mention Parliament. Members of Parliament, however, are bound by both Acts if they hold personal data on individuals in the course of activities such as writing to Ministers and

---

35 New criteria under Schedules 2 & 3 allow personal data, including sensitive personal data, to be processed "for the exercise of any functions of either House": see part II(A)2 above

36 s35A reduces the impact of the sixth principle by removing the most important individual rights in cases which involve privilege

carrying out constituency duties, as the doctrine of exclusive cognisance only applies to Members in respect of activities which are "proceedings in Parliament".[37]

As part of its discussion of the meaning of proceedings in Parliament, the Joint Committee on Parliamentary Privilege noted that much of the work of a Member of Parliament today, although part of his duties as a *member* of Parliament, does not constitute parliamentary *proceedings* and are not, therefore, protected by parliamentary privilege:

> This issue arose in 1958 in a case concerning a member, Mr George Strauss. He wrote an allegedly defamatory letter to a minister on a matter he might later have wished to raise in the House, namely, criticism of the purchasing policies of the London Electricity Board. The House resolved by a narrow majority that the letter was not a proceeding in Parliament as it did not relate to anything then before the House.[38]

The Joint Committee concluded that the exceptional degree of protection given by article 9 of the Bill of Rights "should remain confined to the core activities of Parliament, unless a pressing need is shown for an extension".[39] However, the Committee noted that "in the ordinary course a member enjoys qualified privilege at law in respect of his constituency correspondence".

Members will be bound by the *Data Protection Act 1998* when it comes into force on 1 March 2000. They would benefit from the wide-ranging data protection exemptions for parliamentary privilege given by **Schedule 6, para 1** of the current Bill (see previous section), but again, activities such as casework and correspondence with Ministers are not covered by these exemptions.

## 2. A Brief Guide to Members' Responsibilities under the *Data Protection Act 1998*

The *Data Protection Act 1998* will gradually replace the *Data Protection Act 1984*. Both statutes give rights to individuals about whom personal data is recorded[40] on computer (known as data subjects). The account below focuses on Members' responsibilities under

---

37 see part II(A)1 of this paper, above

38 HC 214-I of 1998-99, Op cit, para 104

39 Ibid, para 110

40 the 1998 Act uses the term "processing", which means obtaining, recording or holding the information or data, including, in relation to personal data, obtaining or recording the information to be contained in the data, or carrying out any operation or set of operations on the information or data

the 1998 Act.[41] It is intended to be only a very simple description of a highly complex new law and should not be relied upon as a definitive guide.[42]

**Data and Personal Data**

In addition to information recorded on computer, "data" includes information recorded in manual filing systems and information held in medical records etc (see below). It also includes information recorded *with the intention* that it should be transferred to a computer or manual filing system. Some applications are which have full or partial exemption under the current law, including word-processing and mailing lists, are covered by the 1998 Act.

"Personal" data is defined as data which relate to a living individual who can be identified from those data,[43] and includes any expression of opinion about the individual and any indication of the intentions of the *data controller* (ie. the person who holds the data) or any other person in respect of the individual.

**Individuals' Rights**

The rights bestowed by part II and Schedule 1 of the 1998 Act include:

- the right to have access to personal data
- the right to be notified by the data controller that personal data is being held at the time it is collected, or shortly after, *regardless of whether a request for access is made*
- the right to be notified of the purposes for which the data is being held
- the right, where appropriate, to have the data corrected or deleted
- the right to prevent processing of personal data where this is likely to cause unwarranted damage or distress
- the right to compensation for damage and distress caused by contravention of the Act

**The Data Protection Principles**

Schedule 1 of the Act contains eight data protection principles which must be followed by data controllers:

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless

---

41 the Data Protection Registrar's *Data Protection Guidelines* provide an excellent commentary on the 1984 Act: available at www.dataprotection.gov.uk/

42 for more detail, see *The Data Protection Act 1998: An Introduction* by the Data Protection Registrar, which is also available at www.dataprotection.gov.uk. A more comprehensive guide is likely to be produced when the necessary secondary legislation is in place

43 or from those data and other information which is in the possession of or is likely to come into the possession of, the data controller

a) at least one of the conditions in Schedule 2 is met, and
b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

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

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

6. Personal data shall be processed in accordance with the rights of data subjects under this Act.

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

**Conditions for Processing Personal Data**

The conditions for processing data mentioned in the first principle are, broadly, as follows:[44]

Conditions for processing *any* personal data

1. The data subject has given his or her consent to the processing
2. The processing is necessary
   a) for the performance of a contract to which the data subject is a party, or
   b) for the taking of steps at the request of the data subject with a view to entering into a contract
3. The processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract

[44] subject to the amendments made by **Schedule 6, paras 3 & 4** of the FOI Bill

4. The processing is necessary in order to protect the vital interests of the data subject
5. The processing is necessary
   a) for the administration of justice,
   b) for the exercise of any functions of either House of Parliament
   c) for the exercise of any functions conferred on any person by or under any enactment,
   d) for the exercise of any functions of the Crown, a Minister of the Crown or a government department, or
   e) for the exercise of any other functions of a public nature exercised in the public interest by any person
6. The processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.

Additional conditions for processing sensitive personal data

1. The data subject has given his or her explicit consent to the processing of the personal data.
2. The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment
3. The processing is necessary-
   a) in order to protect the vital interests of the data subject or another person, in a case where-
      i. consent cannot be given by or on behalf of the data subject, or
      ii. the data controller cannot reasonably be expected to obtain the consent of the data subject, or
   b) in order to protect the vital interests of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld
4. The processing-
   a) is carried out in the course of its legitimate activities by any body or association which-
      i. is not established or conducted for profit, and
      ii. exists for political, philosophical, religious or trade-union purposes,
   b) is carried out with appropriate safeguards for the rights and freedoms of data subjects,
   c) relates only to individuals who either are members of the body or association or have regular contact with it in connection with its purposes, and
   d) does not involve disclosure of the personal data to a third party without the consent of the data subject
5. The information contained in the personal data has been made public as a result of steps deliberately taken by the data subject
6. The processing-
   a) is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings),

b) is necessary for the purpose of obtaining legal advice, or
c) is otherwise necessary for the purposes of establishing, exercising or defending legal rights

7. The processing is necessary-
   a) for the administration of justice,
   b) for the exercise of any functions of either House of Parliament
   c) for the exercise of any functions conferred on any person by or under an enactment, or
   d) for the exercise of any functions of the Crown, a Minister of the Crown or a government department
8. The processing is necessary for medical purposes and is undertaken by-
   a) a health professional, or
   b) a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional
9. The processing-
   a) is of sensitive personal data consisting of information as to racial or ethnic origin,
   b) is necessary for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment between persons of different racial or ethnic origins, with a view to enabling such equality to be promoted or maintained, and
   c) is carried out with appropriate safeguards for the rights and freedoms of data subjects

Sensitive personal data includes information as to-

a) the racial or ethnic origin of the data subject,
b) their political opinions,
c) their religious beliefs or other beliefs of a similar nature,
d) whether they are a member of a trade union (within the meaning of *the Trade Union and Labour Relations (Consolidation) Act 1992*),
e) their physical or mental health or condition,
f) their sexual life,
g) the commission or alleged commission by them of any offence, or
h) any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court in such proceedings.

The conditions relating to "the exercise of any functions of either House of Parliament" which are inserted by **Schedule 6, paras 3 and 4** of the current Bill are unlikely to cover all activities undertaken by Members. The Home Secretary may add additional conditions for the processing of sensitive data by statutory instrument. The draft *Data Protection (Processing of Sensitive Personal Data) Order 1999* adds a number of new conditions, and would allow parties registered under the *Registration of Political Parties Act 1998* to process sensitive personal data consisting of information as to individuals' political beliefs (ie canvass returns) under certain conditions. There is no obvious condition in relation to sensitive personal data which would allow the processing of most

"sensitive" casework-related information without the *explicit* consent of the individuals concerned.

**Enforcement**

Individuals will be able to complain to the Data Protection Registrar (to be renamed the Data Protection Commissioner)[45] if their rights are infringed or the data protection principles are not complied with. The Commissioner has a variety of powers of enforcement at her disposal, although she has in the past sought to achieve compliance through agreement rather than by the use of formal powers.

**Manual Records**

The 1998 Act extends the data protection regime to cover certain manual records, referred to in the Act as "relevant filing systems". The definition of manual records contained in section 1 is somewhat opaque:

> "relevant filing system" means any set of information relating to individuals to the extent that, although the information is not processed by means of equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible.

While this will include card index systems, etc, the Act is not intended to cover

> miscellaneous collections of paper about individuals, even if the collections are assembled in a file with the individual's name or other unique identifier on the front, if specific data about the individual cannot be readily extracted from that collection... except by looking at every document

[HL Deb Vol 587, 16.3.98, cc 467-8].

The Act also covers personal files in the fields of health, education, social work and housing; these records are currently covered by separate statutes.

**Exemptions**

Part IV of the 1998 Act contains a number of exemptions from various provisions of the Act which are relevant to the activities of Government departments and official bodies, including:

---

[45] the FOI Bill would rename the Data Protection Commissioner the Information Commissioner

- National security (section 28)
- Crime and taxation (section 29)
- Regulatory activity (section 31)
- Research, history and statistics (section 33)
- Information made available to the public by or under enactment (section 34)
- Disclosures required by law (section 35)
- Parliamentary privilege (section 35A)[46]
- Armed forces (Schedule 7)
- Judicial appointments and honours (Schedule 7)
- Crown employment and Crown or Ministerial appointments (Schedule 7)
- Management forecasts and planning (Schedule 7)
- Negotiations with the data subject (Schedule 7)
- Legal professional privilege (Schedule 7)
- Self incrimination (Schedule 7)
-

As explained above, the new exemption for parliamentary privilege added by **Schedule 6, para 1** of the *Freedom of Information Bill* is only applicable to Members in respect of proceedings in Parliament and not constituency casework, etc.

**Notification**

The use of computerised personal data covered by the 1984 Act must be registered with the Data Protection Registrar/Commissioner. A simplified procedure for registration with the Commissioner, to be known as notification, will be introduced. Manual filing systems which are covered by the Act will be exempt from the notification process but not from the rest of the Act.

**Transitional Arrangements**

There are a range of provisions under which various types of data will be exempt from some or all of the requirements of the new Act for a transitional period. These include processing of personal data which was already under way immediately before 24 October 1998 (the deadline for implementation of the *Data Protection Directive*). During the transitional period, the 1984 Act will continue to apply. The precise terms of the transitional arrangements are complex and in some circumstances it may be simpler to comply with the new Act in full rather than attempting to meet the conditions for the exemption. There are exemptions for, amongst other things, computerised data processing, manual data processing and mailing lists until 23 October 2001. Manual data which was held prior to 24 October 1998 will also enjoy a more limited exemption from the data protection law from 23 October 2001 until 23 October 2007.

---

[46] as inserted by **Schedule 6, para 1** of the FOI Bill

**Members' Activities and the New Law**

The following table gives a highly simplified indication of whether some of the data processing activities carried out by Members are likely to be covered by the *Data Protection Act 1998.*

| **Activity** | **1984 Act applies?** | **1998 Act applies?** | **Comments** |
|---|---|---|---|
| Casework database | ✓ | ✓ | |
| Casework card index | ✗ | ✓ | Transitional arrangements |
| Casework paper files | ✗ | ? | Depends on how file is structured. Transitional arrangements |
| Word-processed correspondence | ✗ | ✓ | |
| Database of party supporters | ✓ | ✓ | Sensitive data conditions in Sch. 3 |
| Mailing lists | (✓) | ✓ | Exemption under 1984 Act in some circumstances. Transitional arrangements under 1998 Act |
| Proceedings in parliament (speeches, etc) | ✗? | (✓) | Wide exemption given by FOI Bill |
| Canvass returns | ✓ if computerised<br>✗ if manual | ✓ | Authority to process this data 7is subject to regulations being made: see p27 |

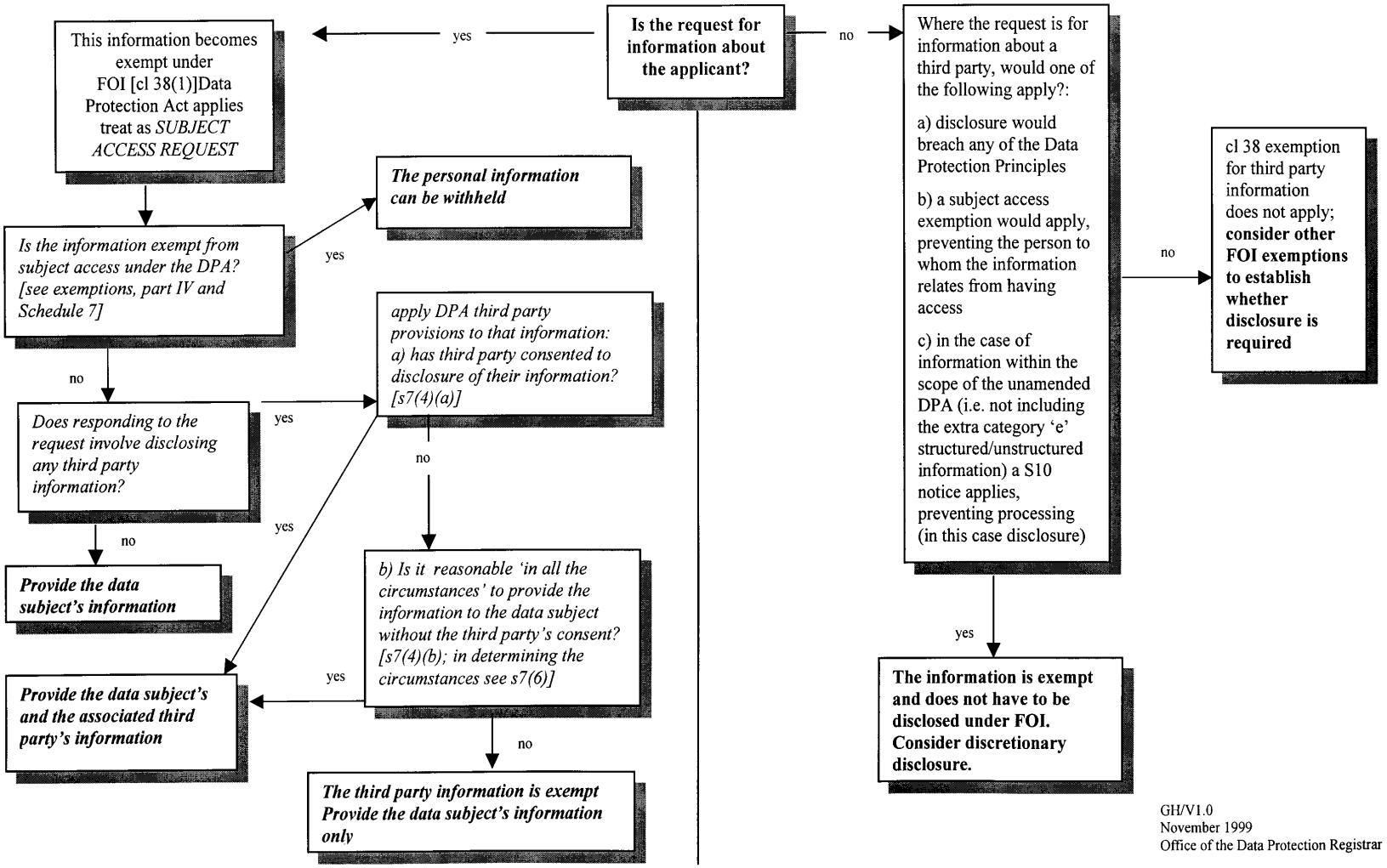
Given the complexity of data protection law and the inherent flexibility of much modern computer software, it is difficult to give definitive general advice on how particular activities are affected by the legislation. Members who are uncertain about how the use of personal data within their Westminster and/or constituency offices are affected can obtain guidance from Samantha Brierley and Charlotte Lewendon of the Data Protection Registrar's office at:

Wycliffe House, Water Lane,
Wilmslow, Cheshire SK9 5AF

**ANNEX: FREEDOM OF INFORMATION BILL**
**PROVISIONS GOVERNING ACCESS TO PERSONAL INFORMATION**
**[DIAGRAM SUPPLIED BY THE DATA PROTECTION REGISTRAR]**

**DATA PROTECTION ACT 1998 (as amended by FOI Act 2000)**

**FOI BILL**




GH/V1.0
November 1999
Office of the Data Protection Registrar