



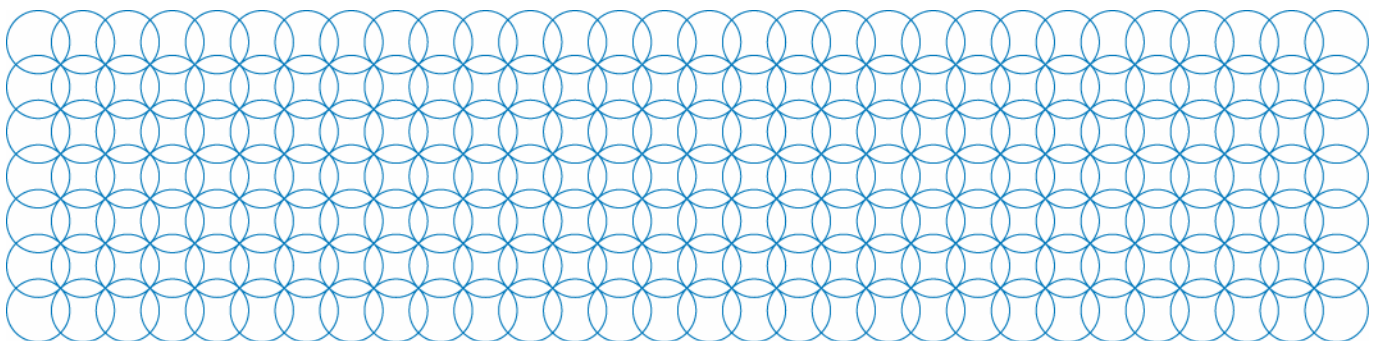
Ministry of
JUSTICE

The Information Commissioner's inspection powers and funding arrangements under the Data Protection Act 1998

Consultation Paper CP(L) 15/08

Published on 16 July 2008

This consultation will end on 27 August 2008





Ministry of
JUSTICE

**The Information Commissioner's inspection
powers and funding arrangements under the
Data Protection Act 1998**

A consultation produced by the Ministry of Justice.

**This information is also available on the Ministry of Justice website:
www.justice.gov.uk**

Contents

Executive summary	7
Introduction	9
Background	14
The Proposals	16
Proposal 1: Promoting Good Practice	17
Proposal 2: Enforcing compliance	21
Proposal 3: Funding	29
About you	35
Contact details/How to respond	36
Impact Assessments	38
The consultation criteria	67

**The Information Commissioner's inspection powers and funding arrangements under the
Data Protection Act 1998 Consultation Paper**

Executive summary

Effective data sharing has come to play a crucial role in improving delivery of public and private sector services. The use of information underpins Government's ability to deliver benefits for the citizen through improved public services, new opportunities for the most disadvantaged, protection from crime and terrorism and sustaining economic well being.

The Information Commissioner (the Commissioner) is the UK's independent regulator of data protection. In performing this role the Commissioner has to balance his duty to educate and promote good practice with his duty to ensure compliance with the Data Protection Act 1998 (DPA). These duties are not mutually exclusive, and should be seen as working together rather than two distinct processes.

This consultation builds on recommendations stemming from the Data Sharing Review recently conducted by Richard Thomas, the Information Commissioner, and Dr Mark Walport, Director of the Wellcome Trust.

A key conclusion of the Data Sharing Review (the Review) was that the Commissioner requires stronger powers and sanctions to carry out his duties as effectively as possible and greater funding to facilitate this.

The Review undertook a comprehensive consultation exercise in formulating their recommendations. In recognition of this, we do not wish to duplicate their efforts. Rather, we wish to seek views on the implementation of proposals based on specific recommendations that are of immediate practical relevance to data controllers and the way they do their job.

Specifically we propose to:

1. Introduce measures to allow data controllers to provide consent to a Good Practice Assessment (GPA) when they register with the Information Commissioner's Office (ICO).
2. Introduce an exemption from section 55A of the DPA, which, on commencement, will create a civil monetary penalty for breaches discovered in the process of a GPA where a data controller has provided prior consent to a GPA.
3. Introduce a three-month notice period for data controllers to withdraw consent for a GPA.

4. Enhance the Commissioner's powers under section 43 of the DPA to enable the Commissioner to specify the time and place that any information should be provided under an Information Notice.
5. strengthen ICO powers under Schedule 9 to enable the Commissioner to demand during an on-site inspection, information reasonably required to determine whether the data controller is complying with the data protection principles.
6. Consider amending Schedule 9 of the DPA to allow the Commissioner to apply for a warrant in cases where he does not have reasonable grounds to suspect a breach of the data protection principles.
7. Introduce a tiered notification fee structure to recognise different sized organisations.
8. Introduce a new sanction for data controllers who knowingly or recklessly provide incorrect information as part of their notification fee self assessment.

Introduction

This paper sets out for consultation proposed changes to the inspection powers and funding arrangements of the Information Commissioner's Office (ICO). The consultation is aimed at organisations and individuals with an interest in the regulation of data protection in the UK, specifically data controllers.

In the main, this consultation is being conducted in accordance with the Code of Practice on Consultation issued by the Cabinet Office and falls within the scope of the Code. The Code of Practice on Consultation notes that "a minimum 12 week consultation process is required during the development of policy". The Code of Practice also says, "however, there will be exceptional circumstances that require a consultation period of less than 12 weeks". Michael Wills MP, Minister of State in the Ministry of Justice, has approved a shorter consultation period of six weeks due to the particular circumstances surrounding this consultation. Events in recent months have demonstrated the pressing need for the Commissioner to acquire new powers to discharge his data protection functions. The Data Sharing Review recently conducted by the Information Commissioner, Richard Thomas, and Dr Mark Walport of the Wellcome Trust, has already consulted broadly on the data protection framework including the powers of the Commissioner and penalties for non-compliance with data protection legislation. Moreover, this consultation is targeted at a specific group, data controllers, and is focussed on proposals that are neither technical nor complex.

Nevertheless, we are making extra efforts to ensure that our consultation is as effective as possible and to ensure all those who wish to, have an opportunity to provide considered input. Events will be held over the coming months to garner views on the recommendations stemming from the Data Sharing Review and the specific issues raised in this consultation document.

Impact Assessments have been completed and form part of this consultation (page 40). Comments on the Impact Assessments are particularly welcome.

Copies of the consultation paper are being sent to:

Association of Chief Executives of Voluntary Organisations

Association of Chief Police Officers in Scotland

Association of Chief Police Officers of England, Wales & Northern Ireland

Association of Private Client Investment Managers & Stockbrokers

Audit Commission

Association of British Insurers

Audit Scotland

British Bankers Association

British Chamber of Commerce

British Insurance Brokers' Association

British Retail consortium

The Cabinet Office

The Campaign for Freedom of Information

CBI Scotland

Central Office of Information

The Charity Commission

Chief Information Officers Council

Citizens Advice Bureau

The Confederation of British Industry

The Consumers' Association

Convention of Scottish Local Authorities

The Customer's Voice

Data Protection Forum

The Department for Business, Enterprise and Regulatory Reform

The Department for Children, Schools and Families

The Department for Communities and Local Government

The Department of Culture, Media and Sport

The Department for Environment, Food and Rural Affairs

The Department of Health

The Department for Innovation, Universities and Skills

The Department for International Development

The Department for Transport

The Department for Work and Pensions

Direct Marketing Association

Experian

Equifax

European Commission

Financial Ombudsman Service

Financial Services Authority

First Minister for Wales, Welsh Ministers and Counsel to the Welsh Assembly

The Foreign and Commonwealth Office

The Forum of Private Business Ltd

FSB Scotland

Foundation for Information Policy Research

General Medical Council

The Home Office

HM Treasury

Information Commissioner's Office (UK)

Information Commissioner's Office (Scotland)

The Information Tribunal

Local Authorities Co-ordinators of Regulatory Services

The Local Government Association

London Investment Bankers Association

Ministry of Defence

National Archives

National Audit Office

The National Association of Data Protection Officers

National Association for Voluntary and Community Action

National Consumer Council

National Council for Voluntary Organisations

National Federation of Self Employed and Small Businesses Ltd

The Northern Ireland Office

Office of National Statistics

Office of Government Commerce

Office of the Scottish Charity Regulator

The Open Rights Group

Privy Council Office

Scottish Council for Development & Industry

Scottish Council for Voluntary Organisations

Scottish Enterprise

The Scottish Government

Scotland Office

The Wales Council for Voluntary Action

Wales Office

The Welsh Assembly Government

Royal Academy of Engineering

Royal College of Pathologists

Royal College of Physicians And Surgeons of Glasgow

Royal College of Physicians of Edinburgh

Royal College of Physicians of London

Royal Pharmaceutical Society of Great Britain

The Wellcome Trust

This list is not meant to be exhaustive nor exclusive and responses are welcomed from anyone with an interest in or views on the subject covered by this paper.

Background

1. The way in which we communicate with one another has developed dramatically and continues to change at a rapid pace. The use of personal information now underpins the provision of both public and private services. In this context it is essential that the management of personal information takes place in a framework and culture that strives not only to provide better services but also to ensure proper respect for individual privacy. The role of the Information Commissioner is key to shaping this culture and environment.
2. In recognition of legal and technological advances in this area the Government initiated a review of the existing data protection framework and how it is used to ensure that personal information has the most robust protection. On 25 October 2007 the Prime Minister announced that he had asked Richard Thomas, the Information Commissioner, and Dr Mark Walport, Director of the Wellcome Trust, to conduct a review of the framework for the use of personal information in the public and private sectors.
3. The Data Sharing Review (the Review) issued a consultation on 12 December, which ran for 2 months and closed having received more than 200 responses. The Review also ran a series of workshops to explore the issues raised in greater detail. The Review's final report was published on Friday 11 July 2008.
4. The Government agrees with the Review that there needs to be a framework put in place to increase public trust and confidence in the handling and processing of personal data by both the public and private sector.
5. Following the announcement of the Review, significant data losses within Government highlighted the need to review data handling procedures within Government. However, further data losses in both the private and public sector have prompted the need to take a comprehensive view of the Information Commissioner's role in ensuring that personal data is handled appropriately.
6. In light of this, we recognise that some of the Review's recommendations require more immediate attention as they are fundamental to ensuring that the benefits of effective data sharing can be realised in an environment where data is handled appropriately. As such, the Government is

conducting this additional consultation exercise on strengthening the Information Commissioner's powers of inspection and funding arrangements for his office. We wish to seek views on the implementation of two specific recommendations in the Review:

- the *Data Sharing Review* Recommendation 12 – that the Commissioner should have a statutory power to gain entry to relevant premises to carry out an inspection, with a corresponding duty on the organisation to co-operate and supply any necessary information. Where entry or co-operation is refused, the Information Commissioner should be required to seek a court order.
 - the *Data Sharing Review* Recommendation 13 – that changes are made to the notification fee through the introduction of a tiered fee system to ensure the regulator receives a significantly higher level of funding to carry out his statutory duties.
7. The Government wants to send a clear signal that the Commissioner can help resolve misunderstanding about compliance, and that data controllers who seek guidance will not be penalised for doing so. However, where data controllers do not seek to comply with the DPA, the Commissioner must have the necessary tools to address this. We have therefore proposed measures designed to complement the Commissioner's existing powers and ensure he has an effective and powerful range of tools to carry out his regulatory functions.

The Proposals

8. The Commissioner is the UK's independent regulator of data protection. In performing this role he has to balance his duty to educate and promote good practice with his duty to enforce compliance with the Data Protection Act 1998 (DPA). The dual nature of the Commissioner's duties should be seen as working together rather than as two isolated processes.
9. The Commissioner is keen to encourage a co-operative approach to data protection. However, where data controllers repeatedly ignore or disregard their regulatory obligations, the Commissioner must have the appropriate tools at his disposal to escalate enforcement action.
10. This balance was echoed in responses to the Data Sharing Review consultation. The Review noted that among other things "the role of the Commissioner and the Information Commissioner's Office (ICO) more generally, was recognised by consultees as being important for educating and influencing the public and organisations, promoting good practice and providing information and advice; resolving complaints from individuals; and enforcing the law by applying legal sanctions against those who ignore or refuse to accept their obligations."¹
11. The DPA provides for a range of important mechanisms to assist the Commissioner in performing his functions. The Review has recommended a number of changes to the regulatory framework and how this is funded to strengthen and complement these existing mechanisms. The Government acknowledges the Review's recommendations in this area and is keen to ensure that the Commissioner has access to an appropriate range of tools and resources to carry out his duties effectively.

¹ Data Sharing Review page 49 paragraph 7.2

Proposal 1: Promoting Good Practice

Encouraging data controllers to come forward for advice

12. Promoting good practice and providing advice on standards are key functions for any regulator. On-site inspections are seen as a particularly useful tool in promoting good practice and providing regulatory advice.²

Current arrangements to assess good practice

13. The Commissioner has the ability to conduct Good Practice Assessments (GPA) under section 51 of the Data Protection Act 1998 (DPA). Section 51(7) of the DPA states:

“The Commissioner may with the consent of the data controller, assess any processing of personal data for the following of good practice and shall inform the data controller of the results of the assessment.”

14. Good practice is given a broad definition under the DPA. It covers practices that are desirable having regard to the data subject's interests, and includes, but is not limited to, compliance with the DPA. The tools the Commissioner can use under this provision are various and are only limited by what the data controller consents to.
15. The GPA is intended as a co-operative process, whereby the Commissioner can work with data controllers to improve standards of compliance and provide advice. A data controller may request an assessment to get the Commissioner's assurance that they are meeting the required standard or to find out how to improve standards. Similarly the Commissioner may want to look at a new or particularly high-risk area of data processing to provide advice on how the DPA applies.
16. The benefits of a GPA are not one-sided. The Commissioner may also use an assessment to learn more about a data controller who is going above and beyond their obligations. These good practice examples can be essential to raising compliance across the board and convincing other data controllers of the benefits of handling personal data well.

² *Reducing Administrative Burdens: effective inspection and enforcement*, Phillip Hampton March 2005.

17. However, if the Commissioner discovers a breach of the DPA in the course of an assessment, he can issue an Enforcement Notice³ to compel a data controller to take measures to comply with the DPA. Failure to comply with an Enforcement Notice is an offence under the DPA.
18. The GPA is not a power but a tool the Commissioner can use to foster a co-operative environment to raise standards. As such the Commissioner must first obtain the data controller's consent to conduct a GPA. This can be a time-consuming process for both the Commissioner and the data controller. For example both may have a different view as to what a useful assessment should involve and securing agreement can lead to protracted and resource intensive negotiations.
19. The DPA requires data controllers to register with the ICO to notify their intention to process personal information.⁴ This process provides an opportunity to streamline the consent process for a GPA.

Making it easier to provide consent for a GPA

20. The Government proposes to put in place measures to allow data controllers to provide their consent for an assessment when they register with the ICO. The Commissioner would be expected to set out what a standard assessment would entail, which is what the data controller would be providing consent to at the point of registration. Of course both the data controller and the Commissioner could negotiate additional terms, but all data controllers would be clear on the scope of a standard assessment.
21. To minimise the likelihood of data controllers providing consent when they register, only to withdraw it when the Commissioner recommends a GPA, we also propose a three-month notice period for data controllers to withdraw their consent. This would not be a statutory notification, however the data controller would be asked to agree to these terms when he or she registers with the ICO.

³ Section 40 of the DPA provides for the Commissioner to issue an Enforcement Notice to compel a data controller to process or cease processing in order to comply with the data protection principles. The Notice must specify what the data controller must do, or cease doing to comply with the relevant requirements of the Act. The Notice may be appealed to the Information Tribunal which may confirm, amend or overturn it. If the data controller fails to comply with a Notice (in absence of an appeal against the Notice) a criminal offence is committed.

⁴ Section 17 of the DPA requires data controllers to register with the Information Commissioner their intention to process personal data. It is a criminal offence to process personal data if the data controller is not registered and not exempt from registration.

22. Under this proposal the fact that a data controller provides consent for a GPA would not necessarily mean that the Commissioner would conduct an assessment of that data controller. Nor would it prevent the data controller from specifically requesting a GPA. Similarly, if the data controller did not provide consent when they register with the ICO there would be nothing to prevent them giving consent at a later date.

Encouraging data controllers to volunteer consent for assessments

23. Government recognises the importance of GPAs to good regulatory practice and to the Commissioner's ability to foster compliance across the board. Accordingly, we propose to offer an incentive to encourage data controllers to provide prior consent for a GPA. Government considers that data controllers who are committed to the appropriate handling of personal data, but who are unclear of their obligations under the Act, should not be penalised for seeking advice or guidance.
24. On commencement of section 55A⁵ of the DPA, the Commissioner will be able to issue a civil monetary penalty for serious breaches of the data protection principles of a kind likely to cause substantial damage or distress. Section 55A will apply in cases of deliberate breach and where a data controller is aware that there is risk of serious breach but fails to take reasonable steps to prevent such a breach.
25. As an incentive for data controllers to provide prior consent for a GPA, Government proposes that those who provide such consent should be given protection from the civil monetary penalty under section 55A. We propose that the Commissioner should not be able to issue a civil monetary penalty in respect of any breaches of the DPA that are discovered in the process of a GPA.
26. We are not proposing to provide any protection from prosecution in relation to criminal offences that might be discovered during a GPA, nor do we propose to protect data controllers from other enforcement action. The Commissioner would be able to employ the remainder of his enforcement tools as required, for example, Enforcement Notices under section 40 of the DPA. In practice, we propose that the Commissioner would not apply a civil monetary penalty for breaches discovered during a GPA, but could issue an Enforcement Notice to compel compliance with the DPA. Should a data controller fail to comply with an Enforcement Notice, he or she

⁵ Section 55A was inserted into the DPA by Section 144 of the Criminal Justice & Immigration Act 2008. It is not yet in force.

would be guilty of an offence under the DPA and the Commissioner would pursue the appropriate action.

27. Our proposal does not affect the rights afforded to data subjects under the Act. Data subjects who have suffered damage as a result of a breach by a data controller would still be able to claim compensation as provided under section 13 of the DPA.

Summary: Proposals to promote good practice

We propose to introduce:

- measures to allow data controllers to provide consent to a Good Practice Assessment when they register with the Information Commissioner's Office
- a three-month notice period for data controllers to withdraw consent for a Good Practice Assessment
- exemption from a civil monetary penalty for breaches discovered in the process of a Good Practice Assessment

Question 1

Do you agree that data controllers should have the opportunity to provide consent for a Good Practice Assessment when registering with the Information Commissioner's Office?

Question 2

Do you agree with the proposed three-month notice period for data controllers to withdraw consent for a Good Practice Assessment?

Question 3

Do you agree with the proposal to exempt data controllers who consent to a Good Practice Assessment from the civil monetary penalty under section 55A of the Data Protection Act 1998 (once in force) for a breach discovered in the process of a Good Practice Assessment? Please give reasons for your answer.

Proposal 2: Enforcing compliance

Enhancing the Commissioner's inspection powers

28. Government considers that effective regulatory action sends a clear signal to all data controllers that the Commissioner can and will take appropriate action to ensure compliance with the DPA. The impact of strong regulatory signals may be enhanced if a data controller believes that their standard of compliance could be reviewed at any time. This can include undertaking assessments or inspections to identify problems and enforce compliance with the DPA.
29. The Review reiterates this point stating “the key to effective enforcement lies in the regulator’s ability to undertake necessary investigations and inspections, so that regulatory failures can be identified and corrected. The possibility or threat of external scrutiny will do much to encourage organisations, in the public, private and voluntary sectors to take compliance seriously”.⁶

Current provisions enabling the Commissioner to request information

30. The DPA provides the Commissioner with tools to support him in carrying out assessments of compliance.
31. The Commissioner and his office are committed to working co-operatively with data controllers and will always make great effort to obtain information without having to resort to using powers under the DPA. Usually the Commissioner will make an initial approach to a data controller to request information informally. Where the data controller chooses not to co-operate the Commissioner will escalate his actions. For example he may write to the data controller, setting out his powers under the DPA and his proposed next steps if the data controller continues to unreasonably refuse to provide the information. However, in cases where a data controller simply refuses to co-operate the Commissioner will use his more coercive powers.
32. Under section 43 of the DPA, following a request from a data subject, or where the Commissioner reasonably requires information for the purpose of determining compliance with the data protection principles, the Commissioner can issue a data controller with an Information Notice. An Information Notice can require a data controller to provide the Commissioner with specified information, in a specified form, to assess

⁶ Data Sharing Review page 66 paragraph 8.61

compliance with the data protection principles. Failure to comply with an Information Notice is a criminal offence under the DPA.

33. The Information Notice gives the Commissioner a power to inspect a data controller's compliance with the data protection principles. This provision empowers the Commissioner to specify the form in which information should be provided, giving substantial scope for its application. The Information Notice does not necessarily allow the Commissioner to go onto a data controller's premises to carry out an inspection, but the Commissioner can require a specific document or an explanation of a data controller's data protection policy and how it is used. The Commissioner could also follow up any request by issuing a further notice requiring an explanation of the information provided.
34. The Commissioner can issue the notice to any data controller as long as he reasonably requires information to determine compliance with the DPA. The Commissioner does not have to suspect a breach of the DPA in order to exercise his powers under section 43, and in practice the Commissioner could issue an Information Notice to randomly audit a data controller. However, any random check would need to be balanced against the principles of good regulatory practice.

Enhancing the Commissioner's powers under section 43

35. While the Commissioner can set a deadline by which information should be provided under section 43, there is no explicit power to specify the manner in which any information should be provided, such as the time or the place. This is essential in situations where the information that the Commissioner requires cannot be easily or securely sent to his office or he needs the data controller to provide the information quickly and in person.
36. Government proposes to enhance the Commissioner's powers under section 43 to be able to specify the time and place that any information should be provided to the Commissioner. This would allow the Commissioner to serve an Information Notice on a data controller, for example, requesting them to provide an explanation of their data security procedure at 10.00am at the data controller's premises. Similarly the Commissioner could require the data controller to attend the ICO to provide the requested information.
37. This proposal would provide the Commissioner with enhanced powers to gather information if he felt that a data controller was attempting to avoid providing the requested information. For example, the Commissioner may request information on how data security measures were exercised on a new database, and in response the data controller could send a copy of a data security manual. However, the Commissioner may require an

explanation of procedures and how they are used in practice. If the data controller refused to provide this information, in effect hiding the true nature of how the database was operated, the Commissioner could require the data controller to attend a meeting to talk through procedures.

38. The Commissioner is committed to working co-operatively with data controllers and ensuring that data controllers are not subject to unnecessary administrative burdens. In practice the Commissioner would be expected to exercise any new powers in a proportionate and reasonable way.

Undertaking an on-site inspection without consent

39. There are occasions where the Commissioner may need to go onto premises to undertake an inspection. While obtaining consent for an inspection is preferred, it may be necessary in some circumstances for the Commissioner to carry out an inspection without consent in order to carry out his duties. This is a separate and more coercive power than requesting or obtaining information by way of an Information Notice.
40. The Review expressed particular concern with the scope of the Commissioner's powers in this area. The Review considers it an "anomaly that there is at present no explicit power requiring a data controller to submit to the scrutiny of an independent inspector or auditor". In particular their concerns focus on the Commissioner's ability to enter premises to undertake inspection.
41. In particular, the Review considers that in practice the existence of a power that provides for the Commissioner to enter a data controller's premises to inspect for compliance with the DPA would do a great deal to raise compliance across the board.
42. The Review goes on to say "the threat of enforced inspection should be sufficient to secure the co-operation of most organisations that come to the regulator's attention, but prove to be recalcitrant. The threat must be real and credible. However, the power to enter premises is strong one and safeguards are essential".

Existing powers of entry

43. The DPA provides the Commissioner with two explicit powers to enter a data controller's premises.

Section 54A Inspection of overseas information systems

44. Under section 54A the Commissioner can enter a data controller's premises to inspect any personal data recorded in the Schengen

Information System the Europol Information System and the Customs Information System. These powers for the Commissioner emanate from the respective EU instruments establishing these systems. National supervisory bodies in other Member States enjoy similar powers.

45. Before exercising this power the Commissioner is required to give written notice of his intentions to the data controller unless the case is one of urgency. Once on the premises the Commissioner can inspect, operate and test equipment that is used for the purpose of processing personal data. Anyone, who obstructs or fails without reasonable excuse to provide assistance in the course of such an inspection, is guilty of an offence under the DPA⁷.

Section 50 and Schedule 9 power of entry with warrant

46. Section 50 and Schedule 9 of the DPA provide the Commissioner with the power to apply to a judge for a warrant to enter premises without consent. Before issuing a warrant the judge must be satisfied that the Commissioner:

- has reasonable grounds for suspecting that a data controller has breached or is breaching the data protection principles, or that an offence has been committed under the Act
- has given the data controller seven days written notice of a search, and requested entry at a reasonable hour and been unreasonably refused, or been granted access but the occupier has unreasonably refused to comply with a request made by the Commissioner.

47. The Commissioner can use reasonable force to enter premises with a warrant. Once on the premises the Commissioner can:

- search the premises
- inspect, examine, operate and test any equipment used for processing personal data
- inspect and seize any documents or other material found on the premises.

48. Attempting to obstruct or failing to provide assistance as reasonably required is a criminal offence. The Schedule 9 warrant provides the Commissioner with a robust power of entry to search premises. The power of entry under this provision is not limited to obtaining evidence of criminal

⁷ Section 60 of the Data Protection Act provides for penalties following prosecution. A person guilty of an offence under the DPA is liable on summary conviction to a fine not exceeding the statutory maximum or on conviction on indictment to a fine.

offences under the Act. The warrant can also be used to obtain evidence of a breach of the data protection principles. The Commissioner is not required to give notice of his intention to search under warrant if he is satisfied that the case is one of urgency or where it would defeat the purpose of entry.

49. This is a powerful provision and as such is likely to be used only in the most serious cases, where data controllers repeatedly refuse to co-operate and show no intention of complying with the data protection principles.
50. Given the coercive nature of the power provided under a warrant and the potential interference with ECHR rights to private life and the enjoyment of private property⁸, judicial oversight is provided.

Data Sharing Review's recommendation on power of entry

51. The Review acknowledges that the Commissioner can enter premises with a warrant. However, the authors expressed concerns with the existing power entry, and considered that the benefits of using a warrant to raise standards were limited.
52. In light of these considerations the Review recommends, in addition to the existing power of entry, that the Commissioner should have an additional power to apply to the Courts for an order to enter premises if:
 - the Commissioner suspects that an organisation is not complying with the law
 - the activities or circumstances are such that there may be a risk of non-compliance even though there are not yet grounds for suspicion
 - the Commissioner needs or wishes to undertake a random check.
53. Once on the premises, the Review recommended that the Commissioner should have the power to:
 - enter the premises
 - require the organisation or its staff to help in obtaining access to data and to provide any related information
 - inspect and copy any information, and

⁸ Article 8 of the ECHR provides a right to respect for private and family life, home and correspondence. Article 1 of Protocol 1 to the ECHR provides a right to the protection of property. This has three parts to it: (a) a natural or legal person is entitled to the peaceful enjoyment of his possessions (b) no one is to be deprived of possessions except in the circumstances described and (c) the state can control use of property in the circumstances described.

- require the organisation or its staff to provide information about procedures for complying with the Act, sources of data, purposes for which personal data are kept, persons to whom data are disclosed and data equipment on the premises.
54. Essentially the proposed power differs from the Commissioner's existing powers in three fundamental ways:
- the introduction of a requirement to assess the risk of non-compliance (or a risk assessment) as grounds for gaining entry,
 - the ability for the Commissioner to enter premises with no grounds, and
 - greater powers to request information under warrant.

Proposal to enhance the Commissioner's powers under Schedule 9

Applying for a warrant with no grounds for suspecting a breach

55. Currently a judge must be satisfied that the Commissioner has reasonable grounds for suspecting a breach has occurred or is occurring before he will issue a warrant under Schedule 9 of the DPA. The Review maintains that this requirement restricts the use of a warrant as a tool for random audits, which they argue, is essential for raising standards across the board.
56. The Review's proposed power would allow the Commissioner to enter a data controller's premises with a court order to undertake a random audit of compliance with the DPA. Government appreciates that such a power of entry could send a strong signal to data controllers that the Commissioner could review their compliance with the data protection principles at any time. Government recognises that this threat could send a powerful message to all data controllers and raise compliance across the board.
57. However, we have reservations about this approach as it places a greater burden on data controllers and raises questions of necessity and proportionality of regulatory response. We consider that this proposal would run contrary to good regulatory practices as outlined in the Hampton Review 2005, more specifically, that inspection programmes should be designed as targeted interventions and that "no inspection should take place without a reason".

Applying for a warrant on the basis of a risk assessment

58. Government recognises that there is a difference between randomly selecting organisations with minimal consideration and those based on a set of selection criteria. The use of random inspections has long been

recognised as unhelpful in regulatory activity⁹, because they can waste scarce resource, by targeting organisations that are complying with the law.

59. Using risk assessments in regulatory activity is recognised as being in line with good regulatory practice and a useful way to target limited resources to high-risk areas. The Hampton Review 2005 recommends that “all regulatory activity should be on the basis of a clear, comprehensive risk assessment”.
60. The Hampton Review 2005 also found that there was “a general acceptance among business and regulators that inspections are an inefficient enforcement mechanism in lower-risk or high-performing businesses, and that risk assessments should inform the work programmes of Inspectorates”.
61. Introducing a risk-based approach in exercising the Commissioner's powers of inspection would allow for an element of randomness that would help to raise standards across the board, but would be exercised within a consistent and transparent framework.
62. Government considers that the Commissioner should only apply to the court for a warrant on the basis of a risk assessment. Completing the risk assessment would help to identify data controllers who were unlikely to be complying with standards but also those engaged in high-risk processing. The Commissioner would be expected to provide statutory guidance on how the proposed power would work in practice, setting out the detail of what he would consider as part of a risk assessment.
63. In order to enhance the Commissioner's power of entry under a Schedule 9 warrant, Government is seeking views on the proposal to allow the Commissioner to apply for a warrant where he reasonably requires access to premises to determine whether a data controller has complied or is complying with the data protection principles. In practice this would require the Commissioner to undertake a risk assessment prior to applying to the courts, so that he can explain to the court why he needs to use the power.

Greater powers to request information while executing a warrant

64. Currently the DPA does not provide the Commissioner with explicit powers to request an explanation of any information he finds during an on-site inspection or investigation. Reviewing documents or testing systems may sometimes provide only part of the picture, and could limit the Commissioner's ability to understand the true nature of data processing

⁹ *Reducing Administrative Burdens: effective inspection and enforcement*, Phillip Hampton March 2005.

within an organisation. For example, a copy of a data protection procedure policy means little if the Commissioner cannot ascertain whether employees are aware of the policy and the extent to which it is actually used.

65. In view of this, and in recognition of the Review's recommendation, Government proposes that the Commissioner's powers under a Schedule 9 warrant be enhanced to allow him to access additional information. Under this proposal, the Commissioner may require any person on the premises where a warrant is being executed to provide the Commissioner with any information he reasonably requires for the purpose of determining whether the data controller has complied with or is complying with the data protection principles. This would allow the Commissioner to request information in the form of an explanation.
66. In addition the proposed provision would provide a broader power to request information from staff as well as data controllers, which could for example include an explanation of any information provided.

Summary: Proposals to enforce compliance

We propose to:

- enhance ICO powers under section 43 for the Commissioner to specify the time and place that any information should be provided under an Information Notice
- consider amending Schedule 9 of the DPA to allow the Commissioner to apply for a warrant in cases where he does not have reasonable grounds to suspect a breach of the data protection principles.
- consider amending Schedule 9 of the DPA to allow the Commissioner to apply for a warrant in cases where he does not have reasonable grounds to suspect a breach of the data protection principles but has undertaken a risk assessment which has identified an organisation as 'high-risk'.
- strengthen ICO powers under Schedule 9 to enable the Commissioner to demand during an on-site inspection, information reasonably required to determine whether the data controller is complying with the data protection principles.

Question 4

Do you agree that when the Commissioner issues an Information Notice, under section 43 of the Data Protection Act 1998 he should have the power to specify the time and place that information should be provided to him? Please give reasons for your answer.

Question 5

Do you agree that the Information Commissioner should be able to enter a data controllers' premises under a court warrant to undertake an inspection in circumstances where,

- a) he does not have reason to suspect non-compliance or a breach of the data protection principles?
- b) he does not have reason to suspect non-compliance or a breach of the data protection principles but has completed a risk-assessment which identifies the data controller as high-risk?

Please give reasons for your answer.

Question 6

Do you agree that the Information Commissioner should have the power to require any person on the premises, where a warrant is being executed, to provide the Commissioner with any information required to determine whether the data controller has complied with or is complying with the data protection principles? Please give reasons for your answer.

Proposal 3: Funding

Amending the structure for funding the Information Commissioner's data protection duties

67. To fund recent changes to the Commissioner's data protection powers and responsibilities, Government proposes to revise the funding structure.

Current funding arrangements of the ICO

68. Notification fees paid by data controllers when registering with the Commissioner fund his data protection responsibilities. The ICO uses this information to maintain a publicly available register of data controllers, which acts as a mechanism for ensuring public transparency and accountability.

69. The notification fee is currently £35 per annum, per data controller and applies to all organisations, not currently exempted from payment of the fee, which process personal information, regardless of nature or size. In 2006-07 the revenue raised through the notification fee was £10.2 million.

Proposed new funding arrangements of the ICO

70. Government proposes to introduce a new funding structure for the ICO to ensure it is appropriately resourced to undertake any additional data protection responsibilities. In accordance with Better Regulation Executive guidance, Government proposes to exempt from payment some smaller organisations. Government also proposes, in order to more accurately represent the level of regulatory activity that may be required under the DPA, to increase the fee for larger organisations and larger public sector bodies to up to £1000.

71. The House of Commons Justice Committee Report *Protection of Private Data*, published on 3 January 2008, notes as an anomaly that all data controllers regardless of size or level of processing pay the same £35 fee. The Committee considered that a "graduated rate would be more appropriate, more likely to reflect actual costs, and more suited to providing an adequate income for the policing of data protection". The Review also recommended a tiered notification fee structure.

72. The Government agrees with this view and proposes a revised tiered notification fee structure based on the size of the organisation. A tiered notification fee structure would address the inequity in the current fee arrangement where individual persons processing data for a few people pay the same amount as a large company or Government Department processing data on millions of people.

73. Government proposes that data controllers undertake a self-assessment process to nominate which tier they fall within based on specified criteria relating to an organisation's size. Government does not consider it necessary or beneficial that the Commissioner make this assessment. We propose to use the existing EU definitions¹⁰ of small, medium and large enterprises to define the notification fee tiers.

74. The ICO currently envisages removing any data controller from the register for fraudulent classification for fee assessment purposes, therefore committing the offence of processing data without correctly registering. However, Government will give consideration to whether it would be appropriate for the introduction of an additional penalty for data controllers who deliberately provide incorrect information as part of their notification fee self assessment and fail to pay the correct notification fee.

Summary: Proposal to amend the structure for funding the Information Commissioner's duties

We propose to:

- introduce a tiered notification fee structure to ensure the extent of regulatory activity required by the ICO is reflected more accurately in the level of notification.
- introduce an additional penalty for data controllers who knowingly and deliberately provide incorrect information as part of their notification fee self assessment.

Question 7

Do you agree with the proposal to introduce a tiered notification fee structure to ensure the extent of regulatory activity required by the ICO is reflected more accurately in the level of notification? Please give reasons for your response.

Question 8

Do you consider it proportionate and appropriate that there should be an additional penalty, other than removal from the register, for data controllers who knowingly and deliberately provide incorrect information as part of their notification fee self assessment?

¹⁰ Department for Business Enterprise and Regulatory Reform, *Thresholds for small and Medium-sized Companies and Groups*, URN No: 05/1973.

Summary Questionnaire

We would welcome responses to the following questions set out in this consultation paper.

Question 1

Do you agree that data controllers should have the opportunity to provide consent for a Good Practice Assessment when registering with the Information Commissioner's Office?

Question 2

Do you agree with the proposed three-month notice period for data controllers to withdraw consent for a Good Practice Assessment?

Question 3

Do you agree with the proposal to exempt data controllers who consent to a Good Practice Assessment from the civil monetary penalty under section 55A of the Data Protection Act 1998 (once in force) for a breach discovered in the process of a Good Practice Assessment? Please give reasons for your answer.

Question 4

Do you agree that when the Commissioner issues an Information Notice under section 43 of the Data Protection Act 1998 he should have the power to specify the time and place that information should be provided to him? Please give reasons for your answer.

Question 5

Do you agree that the Information Commissioner should be able to enter a data controllers' premises under a court warrant to undertake an inspection in circumstances where,

- a) he does not have reason to suspect non-compliance or a breach of the data protection principles?
- b) he does not have reason to suspect non-compliance or a breach of the data protection principles but has completed a risk-assessment which identifies the data controller as high-risk?

Please give reasons for your answer.

Question 6

Do you agree that the Information Commissioner should have the power to require any person on the premises, where a warrant is being executed, to provide the Commissioner with any information required to determine whether the data controller has complied with or is complying with the data protection principles? Please give reasons for your answer.

Question 7

Do you agree with the proposal to introduce a tiered notification fee structure to ensure the extent of regulatory activity required by the ICO is reflected more accurately in the level of notification? Please give reasons for your response.

Question 8

Do you consider it proportionate and appropriate that there should be an additional penalty, other than removal from the register, for data controllers who knowingly and deliberately provide incorrect information as part of their notification fee self assessment? Please give reasons for your response.

Thank you for participating in this consultation exercise.

Glossary

Data controller: a person, who determines the purposes for which, and the manner in which, personal information is to be processed. This may be an individual or an organisation and the processing may be carried out jointly or in common with other persons.

Data subject: the living individual who is the subject of the personal information (data).

Enforcement notice: is issued by the Commissioner if he is satisfied that a data controller has contravened or is contravening the data protection principles. The notice sets out the steps that the data controller must take to comply with the relevant requirements of the Act. The notice may be appealed to the Information Tribunal, which may confirm, amend or overturn it. However, in the absence of an appeal, if the data controller fails to comply with a notice a criminal offence is committed.

Information notice: is a written notice from the Commissioner to a data controller or a public authority seeking information that the Commissioner needs to carry out his functions. Failure to comply with an information notice is an offence.

Notification: is the process by which a data controller's processing details are added to a register. Under the Data Protection Act every data controller who is processing personal information needs to notify unless they are exempt. Failure to notify is a criminal offence. Even if a data controller is exempt from notification, they must still comply with the data protection principles.

Personal data: is information about a living individual who can be identified from that information and other information which is in, or likely to come into, the data controller's possession

Processing: is obtaining, recording or holding the data or carrying out any operation or set of operations on data.

About you

Please use this section to tell us about yourself

Full name	
Job title or capacity in which you are responding to this consultation exercise (e.g. member of the public etc.)	
Date	
Company name/organisation (if applicable):	
Address	
Postcode	
If you would like us to acknowledge receipt of your response, please tick this box	<input type="checkbox"/> (please tick box)
Address to which the acknowledgement should be sent, if different from above	

If you are a representative of a group, please tell us the name of the group and give a summary of the people or organisations that you represent.

Contact details/How to respond

Please send your response by 27 August 2008 to:

Matthew Benson

**Ministry of Justice
Information Rights Division
6th Floor
Selborne House
54-60 Victoria Street
London
SW1E 6QW
Tel: 020 7210 8072
Fax: 020 7210 8388
Email: matthew.benson@justice.gsi.gov.uk**

Extra copies

Further paper copies of this consultation can be obtained from this address and it is also available on-line at <http://www.justice.gov.uk/index.htm>.

Alternative format versions of this publication can be requested from Matthew Benson.

Publication of response

A paper summarising the responses to this consultation will be published within three months of the closing date of the consultation. The response paper will be available on-line at <http://www.justice.gov.uk/index.htm>.

Representative groups

Representative groups are asked to give a summary of the people and organisations they represent when they respond.

Confidentiality

Information provided in response to this consultation, including personal information, may be published or disclosed in accordance with the access to information regimes (these are primarily the Freedom of Information Act 2000 (FOIA), the Data Protection Act 1998 (DPA) and the Environmental Information Regulations 2004).

If you want the information that you provide to be treated as confidential, please be aware that, under the FOIA, there is a statutory Code of Practice with which public authorities must comply and which deals, amongst other things, with obligations of confidence. In view of this it would be helpful if you could explain to us why you regard the information you have provided as confidential. If we receive a request for disclosure of the information we will take full account of your explanation, but we cannot give an assurance that confidentiality can be maintained in all circumstances. An automatic confidentiality disclaimer generated by your IT system will not, of itself, be regarded as binding on the Ministry.

The Ministry will process your personal data in accordance with the DPA and in the majority of circumstances, this will mean that your personal data will not be disclosed to third parties.

Impact Assessments

Summary: Intervention & Options		
Department /Agency: Ministry of Justice	Title: Impact Assessment of Enhancing the Commissioner's Inspection Powers with the Data Protection Act 1998.	
Stage: Partial	Version: 01	Date: 16 July 2008
Related Publications:		

Available to view or download at:

<http://www>

Contact for enquiries: Matthew Benson

Telephone: 020 720 8072

What is the problem under consideration? Why is government intervention necessary?

The Information Commissioner's powers to conduct inspections under the Data Protection Act 1998 (DPA) are important mechanisms for regulating compliance with the data protection principles. Some of the Commissioner's inspection powers are limited, such as the nature of the information he can request during an inspection or investigation. Government intervention is necessary to enhance the Commissioner's powers of external scrutiny to ensure that personal data is processed in compliance with the DPA. This in turn will reduce the likelihood of data losses.

What are the policy objectives and the intended effects?

Effective and secure data sharing among organisations delivers improved public and private services, however recent high profile data breaches have reduced public confidence in this agenda. The policy objective of this proposal is to enhance the Information Commissioner's powers whilst undertaking inspections of compliance with the DPA. This will have the intended effect of identifying and rectifying problems with compliance before they escalate and promote good practice.

What policy options have been considered? Please justify any preferred option.

(1) Retain the status quo; (2) Consider unfettered power of entry to inspect data controllers' systems; (3) Promote good practice and encourage data controllers to come forward for advice and (4) Enforce compliance and enhance the inspection powers of the Information Commissioner. We consider options (3) and (4) to have the most effective impact on encouraging compliance with the DPA.

When will the policy be reviewed to establish the actual costs and benefits and the achievement of the desired effects?

The policy will be reviewed two - three years after implementation.

Ministerial Sign-off For SELECT STAGE Impact Assessments:

I have read the Impact Assessment and I am satisfied that, given the available evidence, it represents a reasonable view of the likely costs, benefits and impact of the leading options.

Signed by the responsible Minister:

.....Date:

Summary: Analysis & Evidence	
Policy Option: 3 & 4	Description: Promoting good practice and encouraging data controllers to come forward for advice Enforcing compliance and enhancing the inspection powers of the Information Commissioner

COSTS	ANNUAL COSTS		Description and scale of key monetised costs by 'main affected groups'
	One-off (Transition)	Yrs	
	£ 2,500,000	1	The costs incurred by the Information Commissioner's Office (ICO) as a result of additional work will be met by a new funding structure. Minimal costs will be incurred by the courts from an increase in the application of Schedule 9 warrants.
	Average Annual Cost (excluding one-off)		
£ 6,000,000		Total Cost (PV) £	
Other key non-monetised costs by 'main affected groups' The costs noted above are not in addition to those noted in the impact assessment on ICO funding. Additional funds raised by the proposal on ICO funding are required to cover the cost of the functions covered in this impact assessment.			

BENEFITS	ANNUAL BENEFITS		Description and scale of key monetised benefits by 'main affected groups'
	One-off	Yrs	
	£ Nil		
	Average Annual Benefit (excluding one-off)		
£ Nil		Total Benefit (PV) £	
Other key non-monetised benefits by 'main affected groups' The main benefit of the proposals is greater compliance by data controllers, leading to fewer data security breaches and greater public confidence in the Government's policy of data sharing.			

Key Assumptions/Sensitivities/Risks A key assumption is that this proposal will ensure that the Commissioner has the appropriate range of tools required to carry out his responsibilities under the DPA, and that enhanced inspection powers will lead to a greater number of inspections carried out by the ICO.

Price Base Year	Time Period Years	Net Benefit Range (NPV) £	NET BENEFIT (NPV Best estimate)
--------------------	----------------------	-------------------------------------	--

What is the geographic coverage of the policy/option?	United Kingdom
On what date will the policy be implemented?	To be confirmed
Which organisation(s) will enforce the policy?	ICO/Civil/Tribunal
What is the total annual cost of enforcement for these organisations?	£ N/A
Does enforcement comply with Hampton principles?	Yes
Will implementation go beyond minimum EU requirements?	Yes

What is the value of the proposed offsetting measure per year?		£ N/A		
What is the value of changes in greenhouse gas emissions?		£ N/A		
Will the proposal have a significant impact on competition?		No		
Annual cost (£-£) per organisation (excluding one-off)	Micro	Small	Medium	Large
Are any of these organisations exempt?	No	No	N/A	N/A

Impact on Admin Burdens Baseline (2005 Prices)				(Increase -
Increase of	£	Decrease of	£	Net Impact
				£

Key: Annual costs and benefits: (Net) Present

Evidence Base (for summary sheets)

The Data Protection Act 1998 (DPA) provides the Information Commissioner with an effective framework under which to regulate the DPA. Nevertheless, the Government recognises that it must continually develop this framework to ensure it keeps pace with advances in the technological and global climates.

The Government proposes to enhance the UK data protection framework by introducing a number of measures:

- (1) **Promoting Good Practice:** Encouraging data controllers to come forward for advice
- (2) **Enforcing Compliance:** Enhancing the Commissioner's inspection powers under the DPA
- (3) **Funding:** Amending the structure for the Information Commissioner's funding arrangements under the Data Protection Act 1998.

This Impact Assessment concentrates on the first and second proposals: promoting good practice and encouraging data controllers to come forward for advice, and enforce compliance by enhancing the Information Commissioner's inspection powers.

Part I: Proposals

Government is putting forward two proposals to enhance the Commissioner's powers of external scrutiny. The first proposal is to encourage the uptake of good practice assessments by both data controllers and the Commissioner. This involves:

- introducing measures to allow data controllers to provide consent to a Good Practice Assessment (GPA) when they register with the Information Commissioner's Office (ICO)
- introducing a three-month notice period for data controllers to withdraw consent for a GPA
- introducing an exemption from the civil monetary penalty under section 55A of the DPA (when it comes into force) for breaches discovered in the process of a GPA where a data controller has provided prior consent to a GPA.

The second proposal is to enhance the Commissioner's inspection powers. This involves:

- enhancing the Commissioner's powers under section 43 for the Commissioner to specify the time and place that any information should be provided under an Information Notice
- considering amending Schedule 9 of the DPA to allow the Commissioner to apply for a warrant in cases where he does not have reasonable grounds to suspect a breach of the data protection principles

- strengthening ICO powers under Schedule 9 to enable the Commissioner to demand, during an on-site inspection, information reasonably required for the purpose of determining whether the data controller is complying with the data protection principles.

Policy objectives and the intended effects

The policy objectives of these proposals are to ensure the Information Commissioner has sufficient powers to undertake inspections of data controllers, and to ensure compliance with data protection principles. Without compulsion, companies will take less than an effective level of care of individuals' data. This will lead to a higher risk of fraud for individuals. Ensuring that data controllers take responsibility for the protection and safety of the data they hold will also serve to strengthen public confidence in the data protection framework.

Rationale for change and reason for Government intervention

Encouraging Good Practice Assessments

The Commissioner has the ability to conduct Good Practice Assessments (GPA) under section 51(7) of the DPA. The GPA is intended as a co-operative process, whereby the Commissioner can work with data controllers to improve standards of compliance and provide advice.

The Commissioner currently undertakes a GPA at the request of the data controller. Alternatively, the Commissioner may select an organisation in high-risk area, for example, where processing involves sensitive data, and request consent for a GPA. In either case the Commissioner must first obtain consent to conduct a GPA, which can be a time-consuming process for both the Commissioner and the data controller.

Government is proposing to enable data controllers to provide their ongoing consent to a GPA when they register with the ICO. All data controllers must register with the ICO on an annual basis in order to be able to process personal data. We consider that providing consent at registration would have a dual benefit of raising awareness amongst data controllers that the GPA exists as well as providing a more efficient consent process.

To minimise the likelihood of data controllers providing consent when they register, only to withdraw it when the Commissioner recommends a GPA, we also propose a three-month notice period for data controllers to withdraw their consent. This would not be a statutory notification, however the data controller would be asked to agree to these terms when he or she registers with the ICO.

As an incentive for data controllers to provide prior consent for a GPA, Government proposes that those who provide such consent should be given protection from the civil monetary penalty under section 55A (which is not yet in force). We propose that the Commissioner should not be able to issue a civil monetary penalty in respect of any breaches of the DPA that are discovered in the process of a GPA.

Enhancing the Commissioner's powers of entry and inspection

Amendment to Section 43 of the DPA

Under section 43 of the DPA, following a request from a data subject, or where the Commissioner reasonably requires information for the purpose of determining compliance with the data protection principles, the Commissioner can issue a data controller with an Information Notice. An Information

Notice can require a data controller to provide the Commissioner with specified information, in a specified form, to assess compliance with the data protection principles. Failure to comply with an Information Notice is a criminal offence under the DPA.

The Information Notice gives the Commissioner a power to inspect a data controller's compliance with the data protection principles. This provision empowers the Commissioner to specify the form in which information should be provided, giving substantial scope for its application. The Information Notice does not necessarily allow the Commissioner to go onto a data controller's premises to carry out an inspection, but the Commissioner can require a specific document or an explanation of a data controller's data protection policy and how it is used. The Commissioner could also follow up any request by issuing a further notice requiring an explanation of the information provided.

Government intervention is required to provide the Commissioner with greater powers to gather information to assess compliance. He may wish to use his powers if he feels that a data controller is attempting to avoid providing information he needs to carry out his duties. While the Commissioner can set a deadline by which information should be provided under section 43, there is no explicit power to specify the time and place that information should be provided to the Commissioner.

We propose to enhance the powers under section 43 to be able to specify the time and place that any information should be provided to the Commissioner. This may also prove useful where the information that the Commissioner requires cannot be easily or securely sent to the Information Commissioner's Office or if the Commissioner needs the data controller to provide the information quickly and in person. In practice, this would allow the Commissioner to serve an Information Notice on a data controller, for example, requesting them to provide an explanation of their data security procedure at 10:00am at the data controller's premises. Similarly the Commissioner could require the data controller to attend the Commissioner premises to provide the requested information.

Increasing powers under Schedule 9 of the DPA

Inspections can provide a strong deterrent to non-compliance, and can be a proactive way to identify and rectify problems before they have a chance to escalate.

The Commissioner has the explicit power to undertake an on-site inspection or assessment in certain circumstances. These circumstances are:

- when a data controller consents to an assessment by the Commissioner for good practice;
- when the Commissioner has reasonable grounds for suspecting the data protection principles are not being complied with and has obtained a search warrant from a judge to conduct an assessment; and
- to assess whether data held in certain international data systems is being processed in accordance with the DPA.

While obtaining consent for an inspection is preferred, it may be necessary in some circumstances for the Commissioner to carry out an inspection without consent in order to carry out his duties. This is a separate and more powerful tool than requesting or obtaining information by way of an Information

Notice. Section 50 and Schedule 9 of the DPA provide the Commissioner with the power to apply to a judge for a warrant to enter and search premises (including inspection and examination of equipment and documents) without consent.

Currently the DPA does not provide the Commissioner with explicit powers to request an explanation of any information he finds during an on-site inspection or investigation. Reviewing documents or testing systems may sometimes provide only part of the picture, and could limit the Commissioner's ability to understand the true nature of data processing within an organisation.

To overcome these issues, Government is proposing to extend the Information Commissioner's powers under a Schedule 9 warrant. Government proposes to extend the Commissioner's powers under Schedule 9 to allow him to require any person on the premises where a warrant is being executed to provide him with any information he reasonably requires for the purpose of determining whether the data controller has complied with or is complying with the data protection principles. This would allow the Commissioner to request information in the form of an explanation.

Government also proposes that the Commissioner should be able to apply to the court for a warrant on the basis of a risk assessment. Completing the risk assessment would help to identify data controllers who were unlikely to be complying with standards but also those engaged in high-risk processing.

A table of the number of warrants that have been applied for by the Information Commissioner over the last few years is at Annex A. It is not expected that this proposed enhanced power will lead to an increase in the number of warrants being issued by the courts, and in most cases the Commissioner will continue to obtain access to information or premises working in co-operation with data controllers.

Proposed amendments to the Data Protection Act

Some of these proposals would require amendments to the DPA, specifically:

- amendment to facilitate an exemption from the civil monetary penalty under section 55A of the DPA (when it comes into force) for breaches discovered in the process of a GPA where a data controller has provided prior consent to a GPA;
- amendment to section 43 to include ability to specify time and place that any information should be provided to the Commissioner in an Information Notice;
- amendment to Schedule 9 to allow the Commissioner to require an explanation of any information found on the premises;
- potential amendments to Schedule 9 of the DPA to allow the Commissioner to apply for a warrant in cases where he does not have reasonable grounds to suspect a breach of the data protection principles, whether or not a risk assessment has been undertaken.

Part II: The policy options that have been considered

- (1) Retain the status quo
- (2) Consider unfettered power of entry
- (3) Encourage the use of good practice assessments
- (4) Amend current legislation to enhance the inspection powers of the Information Commissioner.

We consider, taken together, the proposals under option (3) and (4) will have the most effective impact in ensuring data controllers are fully compliant with the DPA, reducing the likelihood and severity of any future data protection breaches.

Pros, cons and risks of each option

Option 1 – Retain the status quo

The benefit of retaining the status quo is that no new costs would be incurred. However, not doing anything means that there is limited incentive for data controllers to ensure compliance with the DPA. Doing nothing also limits the effectiveness with which the Information Commissioner can conduct inspections.

Option 2 – Consider unfettered power of entry

While a limited number of other regulators have the power to enter premises at any time for the purpose of carrying out their regulatory duties, this generally predates the Human Rights Act 1998 (HRA). The HRA implements Article 8 of the ECHR, which provides a right to respect for private and family life, home and correspondence. For example, the Health and Safety Act 1974 gives local government authorities the power to enter premises at any time for the purpose of carrying into effect any of the relevant statutory provisions; the Competition Act 1988, the Consumer Credit Act 1974, and the Enterprise Act 2002 gives the Office of Fair Trading the power to obtain entry without a warrant in certain circumstances.

The benefits of giving the Information Commissioner an unfettered power of entry is that he will have ultimate powers of entry to inspect the premises of data controllers who he suspects have committed, are committing, or are likely to commit, a breach of the data protection principles. Organisations who are knowingly in breach of the data protection principles would not be able to evade inspection of their data systems and would risk being subject to appropriate enforcement action.

This option carries a significant risk of alienating data controllers rather than encouraging them to work with the Commissioner. Not pursuing this option also carries a risk of data controllers evading investigation by the Commissioner, however we propose to mitigate this risk through other options.

Given the importance of the Commissioner's role to educate and promote good practice, and his preference for a co-operative regulatory environment, we consider the option for unfettered power of entry to premises too extreme.

Option 3 – Encourage the use of good practice assessments

This option provides a more efficient way to gain consent for a good practice assessment, and in turn, facilitates the assessment process. This option encourages data controllers to participate in a GPA, which provides an effective vehicle for education and compliance through co-operation. Data controllers would benefit from targeted guidance from the Commissioner, increasing the standards of data protection.

We do not believe that there are disadvantages to this proposal. One risk of this proposal is that some data controllers who do not provide consent for a good practice assessment may not participate in this process, missing the opportunity to improve their data management systems. This risk exists in the current regulatory environment and is mitigated by the Commissioner's powers to formally investigate compliance with the DPA.

Providing an exemption from the civil monetary penalty under section 55A of the DPA (when it comes into force) for breaches discovered in the process of a GPA, where a data controller has provided prior consent to a GPA, will encourage data controllers who wish to handle data appropriately but aren't sure of their regulatory obligations to come forward for advice. This will result in higher compliance levels and foster good practice.

Option 4 – Enhance the inspection powers of the Information Commissioner

The benefit of this option is that these proposed amendments to the DPA are complimentary to the Commissioner's existing powers, and provide clarity for data controllers and the Commissioner about the extent of information that can be requested throughout an investigation. The proposals to enhance the Commissioner's powers under Schedule 9 will ensure that the Commissioner has access to relevant information in order to carry out his duties and to gain a more accurate understanding of an organisation's compliance with the data protection principles.

This proposal carries a risk of negative feedback from non-compliant organisations, however the Government considers that the Commissioner requires a range of enforcement tools, including the ability to take decisive and strong action where necessary in order to carry out his duties. This option would not affect data controllers who are cooperative and genuinely committed to meeting their regulatory requirements.

Main affected groups

The main group affected by our proposals is data controllers in the UK, including public and private sector organisations. In April 2008, there were 304,551 registered data controllers in the UK.

Analysis of Costs and Benefits

Option 1

This option is cost neutral. No additional costs or benefits would be generated.

Option 2

This option would ensure the Commissioner has easy access to premises of data controllers in order to carry out his duties and provide a powerful incentive to data controllers to comply with their regulatory obligations under the threat of an inspection.

Assuming that this option would only be employed in extraordinary circumstances, there would be minimal costs involved in implementing this proposal. If it were to be used for other purposes, such as random checks of compliance, then costs could include additional resources for the ICO to carry out the inspections.

Government believes that giving the Information Commissioner an unfettered power of entry to inspect systems would not achieve our policy intentions for the following reasons. The Information Commissioner wants to emphasise a cooperative regulatory environment by promoting good practice through education. We also want to ensure that the Commissioner has appropriate powers to enforce compliance, however we consider that an unfettered power of entry would be a disproportionate way to achieve these policy intentions.

Option 3

The costs of this proposal would include additional resources for the ICO in carrying out a greater number of good practice assessments, and costs to data controllers of participating in the assessments. We propose that the ICO costs are met by the Government's proposal to address ICO funding (see separate Impact Assessment).

Businesses are more likely to sign up to these assessments if the costs of doing so are less than the benefits. Whilst there will be additional costs on those organisations who are inspected, in terms of making data/staff available, we believe these costs will be far outweighed by the benefits of an inspection.

The benefits of encouraging good practice assessments are that data controllers will have increased access to advice and guidance from the ICO, relevant to their specific organisation. This would increase compliance and strengthen data security, reducing the likelihood of a breach occurring or the imposition of a fine (when section 55A of the DPA is enacted). This will, in turn, lead to greater customer satisfaction and a safer environment for data sharing.

Option 4

Enhancing the inspection powers of the Information Commissioner will ensure that the Commissioner has access to the information he requires to effectively carry out his duties, particularly where the Commissioner suspects a data controller is trying to evade investigation.

This option would incur costs to the ICO of making inspections and to companies receiving the inspections. We are looking into the funding arrangements of the Information Commissioner's Office for his increased data protection work and this option has been factored into those proposals (see separate Impact Assessment).

There will be some costs for data controllers associated with compliance of Section 43 of the DPA in ensuring that the relevant information is provided to the Information Commissioner, however the only

new aspect of this proposal is for a specific date and time for compliance. The new proposal under Schedule 9 will also have minimal impact for data controllers in terms of providing assistance to the Information Commissioner.

We anticipate that this proposal, in time, will bring about a change in behaviour towards data security for data controllers, increasing compliance and reducing the need for inspections.

There may also be an increase in the number of applications for warrants, however we do not expect this increase to be significant as we do not anticipate a sharp increase in the number of circumstances where the Commissioner would need to escalate his actions to this level. The costs to the judicial system are therefore anticipated to be minimal.

Benefits to this proposal includes greater customer satisfaction, lower levels of fraud and more confident consumers.

Options Conclusion

Given the identified need to address the limitations of the existing data protection framework the Government does not consider it appropriate to do nothing (option 1). We also do not consider that giving the Information Commissioner unfettered access to data controllers' premises (option 2) is an appropriate or proportionate way to achieve improvements in compliance with the data protection principles.

The Government considers that a mix of encouraging good practice (option 3) and enhancing the Commissioner's inspection powers (option 4) will address the needs of the existing framework and help build confidence in the strength of the data protection framework.

Administrative burdens and simplification

Options 1 would not have any additional administrative burdens. Option 2 would incur a burden on data controllers, as they would need to resource the Commissioner's inspection without notice and with little time to arrange cover. An unannounced inspection would disrupt daily business operations. Option 3 implies a small administrative burden for data controllers whereby they will be asked to provide prior consent to a good practice assessment when they register as a data controller with the ICO. We envisage this burden to be minimal. There are no administrative burdens for data controllers in general relating to option 4. For those organisations to which option 4 applies, we consider the burden of providing relevant information about their compliance as appropriate and proportionate to enable the Commissioner to carry out his duties effectively.

Enforcement, sanctions and monitoring

Options (1), (2) (3) or (4) will not have any impact on enforcement.

Competition Assessment

No measurable competition impact is foreseen.

Small Firms Impact Test

Options (1), (2), (3) and (4) have no greater impact on small firms as present.

Legal Aid/Judicial Impact

Options (1), (2), (3) and (4) has no additional impact on legal aid or on the judiciary.

Equality Assessment & Human Rights

These proposals concern data controllers. None of the options considered have any impact on Race, Disability or Gender of individuals. They are compliant with the Human Rights Act.

Public Authorities

Options (1) and (2) would not have any additional impact on public authorities, although there would be an impact on public authorities if they obstructed the Information Commissioner from inspecting their systems and he had a power of entry without a warrant. However, we do not believe that public authorities will be uncooperative with the Information Commissioner. Option (3) or (4) will not have an impact upon Public Authorities unless their systems are being inspected.

Specific Impact Tests: Checklist

Use the table below to demonstrate how broadly you have considered the potential impacts of your policy options.

Ensure that the results of any tests that impact on the cost-benefit analysis are contained within the main evidence base; other results may be annexed.

Type of testing undertaken	<i>Results in Evidence Base?</i>	<i>Results annexed?</i>
Competition Assessment	Yes	No
Small Firms Impact Test	Yes	No
Legal Aid	Yes	No
Sustainable Development	No	No
Carbon Assessment	No	No
Other Environment	No	No
Health Impact Assessment	No	No
Race Equality	Yes	No
Disability Equality	Yes	No
Gender Equality	Yes	No
Human Rights	Yes	No
Rural Proofing	No	No

Annexes

Annex A

Number of warrants applied for by the Information Commissioner, 2005/06-2006/07

Year	No of warrants applied for	% of cases opened
2006/07	7	0.03
2005/06	12	0.05

Summary: Intervention & Options		
Department /Agency: Ministry of Justice	Title: Impact Assessment of amending the funding arrangements for ICO Data Protection Act 1998 work.	
Stage: Partial	Version: 01	Date: 16 July 2008
Related Publications:		

Available to view or download at:
<http://www.>

Contact for enquiries: Matthew Benson

Telephone: 020 7210 8072

What is the problem under consideration? Why is government intervention necessary?

The proposal is to revise the funding structure of the Information Commissioner's Office (ICO) to ensure it is adequately funded to carry out its responsibilities under the Data Protection Act 1998 (DPA) now and in the future. The ICO's costs and responsibilities have increased since the DPA came into force in 2000. The source of the ICO's funding has not increased accordingly, resulting in its resources becoming increasingly stretched. Government intervention is necessary to ensure the ICO is adequately resourced and to provide funding for proposals to increase the ICO's inspection powers.

What are the policy objectives and the intended effects?

The Government aims to revise the funding structure for the ICO from a flat rate fee of £35 per annum, per data controller to a tiered structure based on an organisation's size. This would raise additional funds to enable the ICO to conduct a greater number of inspections and assessments, including ones of greater complexity, to ensure data protection compliance by organisations. The intended outcome is to strengthen public confidence in the UK data protection framework and to exempt smaller organisations from paying a notification fee, which is in accordance with the Better Regulation agenda.

What policy options have been considered? Please justify any preferred option.

(1) Retain status quo; (2) Increase flat rate fee for notification; (3) Introduce a tiered notification fee structure.

The preferred option is (3). This raises the additional funding necessary to enable the ICO to conduct its duties, and addresses the current inequity where small data controllers pay the same fee as large organisations. This also meets the House of Common's Justice Select Committee report 'Protection of Private Data', which concluded a "graduated rate would be more more appropriate" to provide an adequate income for the policing of data protection.

When will the policy be reviewed to establish the actual costs and benefits and the achievement of the desired effects?

The policy will be reviewed two - three years after implementation.

Ministerial Sign-off For SELECT STAGE Impact Assessments:

I have read the Impact Assessment and I am satisfied that, given the available evidence, it represents a reasonable view of the likely costs, benefits and impact of the leading options.

Signed by the responsible Minister:

.....Date:

Summary: Analysis & Evidence	
Policy Option: 3	Description: Introduced a tiered notification fee structure.

COSTS	ANNUAL COSTS		Description and scale of key monetised costs by 'main affected groups'
	One-off (Transition)	Yrs	
	£ 2,500,000	1	
	Average Annual Cost (excluding one-off)		Total Cost (PV) £
£ 6,000,000			
Other key non-monetised costs by 'main affected groups' The one-off costs noted above are required in order to resource the ICO now and in the future, as enabled by the proposals to encourage good practice and enhance the ICO powers of inspection.			

BENEFITS	ANNUAL BENEFITS		Description and scale of key monetised benefits by 'main affected groups'
	One-off	Yrs	
	£ Nil		
	Average Annual Benefit (excluding one-off)		Total Benefit (PV) £
£ 6,000,000			
Other key non-monetised benefits by 'main affected groups' Organisations will have data protection compliant systems, reducing the possibility of data breach. The public will have greater confidence in the Government's data sharing policy.			

Key Assumptions/Sensitivities/Risks
 The main assumption is that this proposal will provide the ICO with the additional required funds to enable the Commissioner to carry out his responsibilities under the DPA.

Price Base Year	Time Period Years	Net Benefit Range (NPV) £	NET BENEFIT (NPV Best estimate) £

What is the geographic coverage of the policy/option?		United Kingdom			
On what date will the policy be implemented?		To be confirmed			
Which organisation(s) will enforce the policy?		ICO/Civil/Tribunal			
What is the total annual cost of enforcement for these organisations?		£ N/A			
Does enforcement comply with Hampton principles?		Yes			
Will implementation go beyond minimum EU requirements?		Yes			
What is the value of the proposed offsetting measure per year?		£ N/A			
What is the value of changes in greenhouse gas emissions?		£ N/A			
Will the proposal have a significant impact on competition?		No			
Annual cost (£-£) per organisation (excluding one-off)		Micro 0	Small TBC	Medium TBC	Large TBC
Are any of these organisations exempt?		Yes	Yes/No	N/A	N/A

Impact on Admin Burdens Baseline (2005 Prices)					(Increase – Decrease)
Increase of	£	Decrease of	£	Net Impact	£

Key: Annual costs and benefits: (Net) Present

Evidence Base (for summary sheets)

The DPA is regulated independently of Government by the ICO. The ICO's main functions are:

- the promotion of good practice – providing information and advice;
- the resolution of problems – complaints from people who feel their rights have been breached; and
- enforcement – using legal sanctions to ensure compliance with data protection obligations.

The DPA provides the ICO with an effective framework under which to regulate the obligations of data controllers. The Government recognises, however, that the UK data protection framework must be continually developed and revised where appropriate to ensure it is fit for purpose.

The House of Common's Justice Select Committee report '*Protection of Private Data*', published on the 3 January 2008, called for an increase in the ICO's powers of inspection, the introduction of an offence for security breaches "where they were reckless or repeated" and a review of the notification fee structure to ensure the ICO has adequate resources to undertake this work. Government agrees and proposes to revise the notification fee structure accordingly.

The Government proposes to enhance the UK data protection framework by introducing a number of measures:

- (4) **Promoting Good Practice:** encouraging data controllers to come forward for advice
- (5) **Enforcing Compliance:** enhancing the Commissioner's inspection powers with the DPA
- (6) **Funding:** amending the structure for funding the ICO's data protection duties.

This impact assessment concentrates on the third proposal for funding.

Part I: Proposal - amendment to the funding structure for ICO's data protection responsibilities

Government proposes to introduce a tiered notification fee structure, providing additional funds for the ICO's data protection responsibilities. This structure would replace the current flat rate notification fee, thereby more accurately reflecting the Government's Better Regulation agenda.

A tiered structure is considered appropriate as it has the benefit of being relatively simple but still allows for different sized organisations to pay a different notification fee based on their size.

ICO research has indicated that larger enterprises, as defined by turnover and number of employees, generally process larger amounts of personal data. Therefore a larger fee for these organisations more accurately represents the level of regulatory activity that may be required under the DPA. For the method of calculation please see **Annex One** below.

Government also proposes that data controllers undertake a self-assessment process to nominate which tier they fall within, based on specified criteria relating to an organisation's size. Government does not consider it necessary or beneficial that the Commissioner make this assessment. We propose to use the existing EU definitions of small, medium and large enterprises to define the notification fee tiers.

The ICO currently envisages removing any data controller from the register for fraudulent classification for fee assessment purposes, therefore committing the offence of processing data without correctly registering. However, Government is giving consideration to whether it would be appropriate for the introduction of an additional penalty for data controllers who deliberately provide incorrect information as part of their notification fee self assessment and fail to pay the correct notification fee.

Once the Ministry of Justice (MOJ) has analysed the responses to this consultation and completed further work on the specific tiers for notification fees, a further impact assessment will be carried out to explore the impact of the tiers on different sized organisations.

Policy objectives

The policy objectives of this funding proposal are to:

- 1 enable the ICO to effectively conduct and enhance its current regulatory functions under the DPA
- 2 enable the ICO to provide the additional functions as noted above
- 3 ensure the extent of a data controller's regulatory activity is reflected accurately by the notification fee payable, thereby more accurately representing the Government's Better Regulation agenda
- 4 strengthen public confidence in the data protection framework
- 5 enable the ICO to recruit and train appropriately skilled staff to investigate complaints of greater complexity

Intended outcomes

The intended outcomes of this proposal are to:

- Enable the ICO to carry out its regulatory functions under the DPA
The ICO currently has the powers to inspect and assess an organisation's compliance with the DPA. An Enforcement Notice is issued where the ICO considers an organisation is not compliant with the DPA, which carries a criminal offence for non-compliance. Inspection has become an increasingly important aspect of the ICO's responsibilities, providing a strong deterrent to non-compliance. Inspection also proactively assists in identifying and rectifying problems before they escalate. Additional funding is needed to enhance the ICO's current duties under the DPA. A table of cases opened by the ICO over recent years is found at **Annex Two** below.
- Enable the ICO to conduct additional functions
A tiered fee structure would allow for additional funding to be raised on an annual basis. This would fund the additional duties of the ICO proposed in this consultation. For a table of the ICO's income receipts over recent years see **Annex Three** below.
- Exempt certain organisations from the notification fee
In accordance with Government's Better Regulation agenda, a tiered structure would allow for exemption from payment of the notification fee for those organisations defined by the BERR standards for exemption. Organisations exempted from payment of the notification fee would still be required to register with the ICO.

- Strengthen public confidence in data protection framework

Additional funding would resource the proposed additional powers of the ICO, which are designed in part to assist in strengthening public confidence in data protection and security. The ICO would have enhanced inspection powers under the DPA, resulting in more inspections and increased compliance levels. The use of the ICO's enhanced powers will send a clear signal to all data controllers that the Commissioner can and will take appropriate action to ensure compliance with the DPA.

- Enable the ICO to recruit and train staff to the required level to investigate complaints of greater complexity

Information technology has significantly advanced since the DPA came into force, and computer systems are becoming increasingly complex. This has resulted in the ICO requiring different levels of expertise and adequately trained specialists to investigate these more complex systems. The additional funding proposed in this consultation would enable the ICO to recruit and train appropriately skilled staff to investigate more complex cases.

Rationale for change and reason for Government intervention

Due to an increased awareness of the ICO's role and service since the DPA came into force in 2000, the workload of the ICO has increased dramatically. This has resulted in the ICO's resources becoming increasingly stretched. The number of cases opened has more than doubled in four years. In order to equip the ICO to carry out its current and future duties, including implementation of the proposed enhanced powers, the Government needs to act to ensure that appropriate funding arrangements are in place. The increase in organisations registered with the ICO is illustrated at **Annex Four** below.

In addition to an increase in the number of cases opened, the complexity of the ICO's workload has increased. This provides a constant challenge for the ICO to keep up with the changing environment, including recruiting and training staff to carry out assessments on increasingly complex cases.

The ICO's responsibilities are currently funded by a flat rate notification fee paid by organisations, regardless of size, under section 18(5) and section 26 of the DPA. There has not been a change to the fee, even to take account of inflation, since the DPA came into force in 2000. A tiered structure would more accurately represent the Government's Better Regulation agenda by allowing for exemption for smaller businesses while at the same time increasing the income from the overall notification fee to ensure the ICO is adequately resourced.

For the Government to restore public faith in its data sharing policy, it must ensure that organisations in both the public and private sectors take responsibility for managing their data more effectively, and to minimise data security breaches in the future. This can only be done by ensuring the ICO has adequate resources to perform its current and future functions.

Main affected groups

Any organisation that processes data will be affected by these proposals. As of April 2008 there were 304,551 data controllers registered on the ICO's public register, ranging from Central Government Departments and their agencies to small private sector businesses. A table on the breakdown of those registered with the ICO by sector is at see **Annex Five** below.

Part II: The policy options that have been considered

- (1) Retain status quo

(2) Increase flat rate fee for notification

(3) Introduce of tiered notification fee structure

The Government's preferred option is option 3, which raises the necessary additional funding, to enable the ICO to conduct current and additional duties while keeping fee increases to a minimum. This option also addresses the Justice Select Committee's view on the current inequity within the notification fee structure whereby an individual data controller processing data on a few people pays the same fee as a large company or Government Departments that may process the personal information of millions.

There has also been a significant rise in the number of organisations registering intent to process personal information with the ICO, which has led to an increase in complaints and investigations.

Option 1 – Retain status quo

There would be no additional financial burden on organisations under this option.

Disadvantages include that there would not be additional funding for the ICO to conduct assessments on a growing number of organisations on its register. There would also not be adequate resources to enable the ICO to enhance its current regulatory functions and there would be limited incentive for smaller organisations not currently registered with the ICO to do so. Under this option the conclusions of the Justice Select Committee regarding the notification fee not being compliant with the Better Regulation agenda would not be addressed.

Risks of this option include the potential limitation of the effectiveness to investigate a larger number of complaints thoroughly, a potential increase in more complex complaints not being adequately investigated, and a potential increase in the risk of data protection breaches.

Option 2 – Increase flat rate fee for notification

The advantages of this option is that it would raise the necessary funding to enable the ICO to enhance its current responsibilities under the DPA, and for the ICO to conduct additional responsibilities under the DPA.

Disadvantages of this option include that the conclusions of the Justice Select Committee regarding the notification fee not being compliant with the Better Regulation agenda would not be addressed. This option would also mean that the risks or actual costs associated with regulating individual data controllers according to their size would not be accurately reflected. An increased flat rate fee for notification would also mean an increased burden on smaller organisations currently registered with the ICO and there would not be an incentive for smaller organisations to register with the ICO.

This option carries the risk that, particularly given the Justice Select Committee conclusions, smaller organisations could feel an increase is unwarranted and disproportionate.

Option 3 – Introduce a tiered notification fee structure

This option has a number of advantages, including:

- the ICO would have adequate funding to conduct assessments on a growing number of organisations on its register

- the ICO would have adequate resources to meet its current and future responsibilities, including the enhanced powers included in this consultation
- there would be an incentive for smaller organisations not currently registered with the ICO to do so, increasing compliance with the DPA
- the conclusions of the Justice Select Committee regarding the notification fee not being compliant with the Better Regulation agenda would be addressed
- the proposed sanction would provide a disincentive for data controllers who try to avoid paying the appropriate notification fee and would encourage data controllers to register correctly.

The disadvantage of this option is that the ICO would need to introduce a new notification fee system resulting in an initial one-off cost of an estimated £1.5 million. This would be recovered via the revised notification fees during the first year. Additional funds would be available to support the ICO from year two onwards.

This option carries the risk that some data controllers may try to avoid paying the higher fees associated with tiers for larger organisations by placing themselves in a lower band when registering with the ICO. The Government considers that the number of organisations who would look to commit fraud in this manner will be limited, however as noted above, we are considering an additional sanction to mitigate this risk.

Analysis of costs and benefits

Option 1

This would be cost neutral, as the status quo would remain. No additional costs or benefits would be generated.

Option 2

An increase in the flat rate fee to £55 for all data controllers would raise the additional funding required and there would not be a need to establish a new notification system. A 'one size fits all' approach, however, does not address the inequities of the existing fee structure.

Option 3

An estimated additional £6million is required to enable the ICO to carry out its current and proposed future duties successfully. The last few years have seen an increase in the number of data controllers registering with the ICO, resulting in an increased workload for the ICO. The steadily increasing work will require additional qualified staff (£0.5m), bigger offices to house additional staff (£0.5m) and the establishment of a tiered notification fee system (£1.5m). All costs will be met from fee increases. Year 2 will therefore see an increased number of assessments and inspections being undertaken by the ICO.

Changing the notification system will bring additional benefits such as enabling online notification, which will result in a more efficient registration process.

Options conclusion

Government considers doing nothing is not a viable option. Similarly option two does not address the inequities of the existing arrangements. Government prefers option three, which will contribute towards

satisfying the public's concerns over the existing data protection framework and provide the necessary funding for the ICO to carry out its current and additional duties.

Administrative burdens and simplification

The requirement for data controllers to register with the ICO will not change under any of the options. The burden of paying the fee will be lifted for those exempted under a tiered structure in accordance with the Government's Better Regulation agenda.

Enforcement, sanctions and monitoring

None of the options will have an effect on enforcement, sanctions or monitoring.

Competition assessment

No measurable competition impact is foreseen on any of the options.

Small firms impact test

Option one will have no more effect on small firms than the existing arrangements. Some small/medium-sized businesses may have to pay marginally higher fees to the ICO for registering their intention to process personal data on option two and three. However, as smaller organisations will be exempt from the fee there will not be any foreseeable financial impact as a result of the proposed change.

Legal aid/judicial impact

None of the options present an impact on legal aid and there will be no judicial impact.

Equality assessment & human rights

The options are compliant with the Human Rights Act, with no impact on race, disability, or gender of individuals.

Public authorities

Option one will have no more impact on public authorities than the existing arrangements. Depending on the size of the public authority, under options two and three, they may have to pay marginally higher fees to the ICO for registering their intention to process personal data. However, smaller organisations will be exempt and there will no financial impact as a result of the proposed change.

Specific Impact Tests: Checklist

Use the table below to demonstrate how broadly you have considered the potential impacts of your policy options.

Ensure that the results of any tests that impact on the cost-benefit analysis are contained within the main evidence base; other results may be annexed.

Type of testing undertaken	<i>Results in Evidence Base?</i>	<i>Results annexed?</i>
Competition Assessment	Yes	No
Small Firms Impact Test	Yes	No
Legal Aid	Yes	No
Sustainable Development	No	No
Carbon Assessment	No	No
Other Environment	No	No
Health Impact Assessment	No	No
Race Equality	Yes	No
Disability Equality	Yes	No
Gender Equality	Yes	No
Human Rights	Yes	No
Rural Proofing	No	No

Annexes

Annex One

Calculation of the notification fee in a tiered structure

The working assumption for calculating any notification fee increase is that:

- the size of the ICO register remains around 300,000 data controllers;
- the funding required for the ICO is £16 million; and
- estimated fee income for 2007/08 is £10,500,000.

Given the above, an additional £5-6 million will need to be raised under the new structure.

The criteria proposed to allocate each data controller a notification fee would be based on the recognised Government and EU definitions for small, medium and large enterprises. Therefore the criteria for allocating a notification fee would be based on the:

- number of employees;
- turnover; and
- balance sheet total.

Work is currently under way to more accurately calculate the proposed tiered fees but the two examples below of how a tiered structure could work give a general indication of the figures being assessed. These examples are only two of many variations that could be adopted to produce the desired income.

Fee	% of data controllers
£0	60%
£80	35%
£500	5%

Fee	% of data controllers
£0	60%
£100	37%
£1000	3%

Annex Two

Cases opened by the ICO, 2003/04-2006/07

Year	No of cases opened
2003/04	11664
2004/05	19460
2005/06	22059
2006/07	23988

Annex Three

ICO income receipts, 2004/05-2007/08

Year	Income from notification fees
2004/05	£9.2m
2005/06	£9.7m
2006/07	£10.2m
2007/08	£10.5m (estimated)

Annex Four

Data controllers registered with the ICO, 2005-2008

Year	Notifications held at the ICO	% increase on previous year
April 2005	258,770	N/A
April 2006	271,669	4.98
April 2007	287,074	5.67
April 2008	304,551	6.09

Annex Five

Approximate breakdown of notification fees paid by sector, 2007

Type of Organisation	Number of notification fees paid
Public Sector	75,000
Private Sector	170,000
Third Sector	13,000
Unknown	44,000

The consultation criteria

The six consultation criteria are as follows:

Consult widely throughout the process, allowing a minimum of 12 weeks for written consultation at least once during the development of the policy.

Be clear about what your proposals are, who may be affected, what questions are being asked and the time scale for responses.

Ensure that your consultation is clear, concise and widely accessible.

Give feedback regarding the responses received and how the consultation process influenced the policy.

Monitor your department's effectiveness at consultation, including through the use of a designated consultation co-ordinator.

Ensure your consultation follows better regulation best practice, including carrying out an Impact Assessment if appropriate.

These criteria must be reproduced within all consultation documents.

Consultation Co-ordinator contact details

If you have any complaints or comments about the consultation **process** rather than about the topic covered by this paper, you should contact Gabrielle Kann, Ministry of Justice Consultation Co-ordinator, on 020 7210 1326, or email her at consultation@justice.gsi.gov.uk.

Alternatively, you may wish to write to the address below:

**Gabrielle Kann
Consultation Co-ordinator
Ministry of Justice
5th Floor Selborne House
54-60 Victoria Street
London
SW1E 6QW**

If your complaints or comments refer to the topic covered by this paper rather than the consultation process, please direct them to the contact given under **the How to respond** section of this paper at page 36.

[leave blank – inside back cover]

