

## Summary: Intervention & Options

**Department /Agency:**

**Ministry of Justice**

**Title:**

**Impact Assessment of Enhancing the Commissioner's Inspection Powers with the Data Protection Act 1998 - Assessment Notices.**

**Stage:** Legislation

**Version:** Draft 4

**Date:** 9 November 2009

**Related Publications:** Consultation Paper and Government Response on the Information Commissioner's Inspection Powers and Funding Arrangements under the Data Protection Act 1998; Coroners and Justice Bill (as introduced to the House of Lords on 26 March 2009); Impact Assessment of introducing tiered notification fees for the Information Commissioner.

**Available to view or download at:**

[www.justice.gov.uk/publications/cp1508.htm](http://www.justice.gov.uk/publications/cp1508.htm)

[services.parliament.uk/bills/2008-09/coronersandjustice.html](http://services.parliament.uk/bills/2008-09/coronersandjustice.html)

**Contact for enquiries:** Ollie Simpson

**Telephone:** 020 3334 4566

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

The Information Commissioner's powers to conduct inspections and assessments under the Data Protection Act 1998 (DPA) are important mechanisms for regulating compliance with the data protection principles. Significant data losses and breaches of the DPA have occurred and continue to occur. Government intervention is necessary to enhance the Commissioner's powers of inspection and investigation to improve his ability to encourage compliance with the DPA, raise overall standards of data protection, and reduce the likelihood of future data breaches.

**What are the policy objectives and the intended effects?**

The objectives are to enhance the Information Commissioner's powers by allowing him to undertake mandatory assessments of data controllers to assess compliance with the DPA. This will have the intended effect of identifying and rectifying problems before they escalate, and of promoting effective and secure processing and sharing of personal data within and amongst organisations, thereby delivering improved public and private services.

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

Three main options have been considered, which are assessed against the 'base case'. Briefly these are :

- i. *Option 1* - Allow the Information Commissioner to carry out mandatory assessments of central government departments and such other public authorities that are designated as liable by Order;
- ii. *Option 2* - Allow the Information Commissioner to carry out mandatory assessments of central government departments and such data controllers (whether in the public or private sector) as are designated as liable by Order;
- iii. *Option 3* - Allow the Information Commissioner to carry out mandatory assessments of all data controllers.

**When will the policy be reviewed to establish the actual costs and benefits and the achievement of the desired effects?** This policy would be reviewed in 5 – 10 years. An evaluation strategy would be prepared to help collect data for monitoring purposes.

**Ministerial Sign-off** For Implementation 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:

Michael Wills

.....Date: 12 November 2009

## Summary: Analysis & Evidence

**Policy Option: 1**

**Description:** Allow the Information Commissioner's Office (ICO) to undertake mandatory assessments of central government departments and such public authorities that are designated as liable by Order

<b>COSTS</b>	<b>ANNUAL COSTS</b>		Description and scale of <b>key monetised costs</b> by 'main affected groups' There would be direct costs to society from additional administrative costs to the ICO estimated at £17.2m. There may also be additional resource burdens on central government departments and public authorities designated as liable by order. These are estimated at £0.63m, assuming 25 annual assessment notices and 70 man-hours burden per case.	
	<b>One-off (Transition)</b>	<b>Yrs</b>		
	£			
	<b>Average Annual Cost (excluding one-off)</b>			
	£		<b>Total Cost (PV)</b>	<b>£ 17.9m</b>
Other <b>key non-monetised costs</b> by 'main affected groups' There may be additional costs to the Information Tribunal as a result of any appeals that may be made in objection to assessment notices being served by the ICO.				

<b>BENEFITS</b>	<b>ANNUAL BENEFITS</b>		Description and scale of <b>key monetised benefits</b> by 'main affected groups' There would be direct benefits to society in terms of swifter correction of data mishandling; increased deterrence effect of the ICO inspection regime; and greater information to the public. The combination of these factors may lead to prevention of data breaches. Assuming at least two cases are prevented this could lead to benefits of around £24.2m	
	<b>One-off</b>	<b>Yrs</b>		
	£ Nil			
	<b>Average Annual Benefit (excluding one-off)</b>			
	£ Nil		<b>Total Benefit (PV)</b>	<b>£ 24.2m</b>
Other <b>key non-monetised benefits</b> by 'main affected groups' There may be additional benefits to the public from increased public confidence in public sector organisations' ability to provide services, especially when those services are applied for voluntarily.				

**Key Assumptions/Sensitivities/Risks** The net present value is sensitive to deterrence benefits assumption; cost of data losses; man hours lost by public sector organisations; ICO assessment notices running costs; and value of working time assumptions.

Price Base Year 2008	Time Period Years 10	<b>Net Benefit Range (NPV)</b> <b>£ - 5.8m - £18.4m</b>	<b>NET BENEFIT (NPV Best estimate)</b> <b>£ 6.3m</b>
-------------------------	-------------------------	--	---

What is the geographic coverage of the policy/option?		United Kingdom	
On what date will the policy be implemented?		c. April 2010	
Which organisation(s) will enforce the policy?		ICO/Courts	
What is the total annual cost of enforcement for these organisations?		£ 2m	
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?	N/A	N/A	N/A    N/A

<b>Impact on Admin Burdens Baseline (2008 Prices)</b>				(Increase -
Increase of	£ 0.63m	Decrease of	£ 0	<b>Net Impact</b> £ 0.63m

Key: Annual costs and benefits: (Net) Present

<b>Policy Option: 2</b>	<b>Description:</b> Allow ICO to undertake mandatory assessments of central government departments, public authorities as designated by order, and all private data controllers who are members of descriptions that are designated as liable by Order ( <i>preferred option</i> )
-------------------------	--

<b>COSTS</b>	<b>ANNUAL COSTS</b>	Description and scale of <b>key monetised costs</b> by 'main affected groups' There would be direct costs to society from additional administrative costs to the ICO estimated at £17.2m. There may also be additional resource burdens on central government departments, and on public and private sector organisations designated as liable by order. These are estimated at £1.3m.
	<b>One-off (Transition)</b> <b>Yrs</b>	
	£	
	<b>Average Annual Cost (excluding one-off)</b>	
£	<b>Total Cost (PV)</b>	<b>£ 18.5m</b>
Other <b>key non-monetised costs</b> by 'main affected groups' There may be additional costs to the Information Tribunal as a result of any appeals that may be made in objection to assessment notices being served by the ICO. There may also be costs on the Courts, as the ICO applies for Schedule 9 warrants where an assessment notice has not been complied with.		

<b>BENEFITS</b>	<b>ANNUAL BENEFITS</b>	Description and scale of <b>key monetised benefits</b> by 'main affected groups' There would be direct benefits to society in terms of swifter correction of data mishandling; increased deterrence effect of the ICO inspection regime; and greater information to the public. The combination of these factors may lead to prevention of mishandling cases. Assuming at least four cases are prevented this could lead to benefits of around £48.3m
	<b>One-off</b> <b>Yrs</b>	
	£	
	<b>Average Annual Benefit (excluding one-off)</b>	
£	<b>Total Benefit (PV)</b>	<b>£ 48.3m</b>
Other <b>key non-monetised benefits</b> by 'main affected groups' There may be additional benefits to the public and to private sector organisations from increased public confidence in their ability to provide goods and services.		

**Key Assumptions/Sensitivities/Risks** The net present value is sensitive to deterrence benefits assumption; cost of data losses; man hours lost by public and private sector organisations; ICO assessment notices running costs; and value of working time assumptions.

Price Base Year 2008	Time Period Years 10	<b>Net Benefit Range (NPV)</b> <b>£ 17.8m - £ 41.9m</b>	<b>NET BENEFIT (NPV Best estimate)</b> <b>£ 29.8m</b>
-------------------------	-------------------------	--	--

What is the geographic coverage of the policy/option?		United Kingdom	
On what date will the policy be implemented?		April 2010	
Which organisation(s) will enforce the policy?		ICO/Courts	
What is the total annual cost of enforcement for these organisations?		£ 2m	
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	Micro	Small	Medium      Large
Are any of these organisations exempt?	No	No	No      No

<b>Impact on Admin Burdens Baseline (2008 Prices)</b>				(Increase -
Increase	£ 1.3m	Decrease of	£ 0	<b>Net Impact</b> <b>£ 1.3m</b>

Key: Annual costs and benefits: (Net) Present

<b>Policy Option: 3</b>	<b>Description:</b> Allow the Information Commissioner to carry out mandatory assessments of all data controllers
-------------------------	---

<b>COSTS</b>	<b>ANNUAL COSTS</b>		Description and scale of <b>key monetised costs</b> by 'main affected groups' There would be direct costs to society from additional administrative costs to the ICO estimated at £17.2m. There may also be additional resource burdens on central government departments, public authorities and private sector organisations subjected to mandatory assessments estimated at £2.5m.
	<b>One-off (Transition)</b>	<b>Yrs</b>	
	£	1	
	<b>Average Annual Cost (excluding one-off)</b>		
£			<b>Total Cost (PV)</b> £ 19.7m

Other **key non-monetised costs** by 'main affected groups' There may be additional costs to Information Tribunal as a result of any appeals that may be made in objection to assessment notices being served by the ICO. There may also be costs on the Courts, as the ICO applies for Schedule 9 warrants where applicable, slightly greater than under Option 2.

<b>BENEFITS</b>	<b>ANNUAL BENEFITS</b>		Description and scale of <b>key monetised benefits</b> by 'main affected groups' There would be direct benefits to society in terms of swifter correction of data mishandling; increased deterrence effect of the ICO inspection regime; and greater information to the public. The combination of these factors may lead to prevention of mishandling cases. Assuming at least eight cases are prevented this could lead to benefits of around £96.7m
	<b>One-off</b>	<b>Yrs</b>	
	£		
	<b>Average Annual Benefit (excluding one-off)</b>		
£			<b>Total Benefit (PV)</b> £ 96.7m

Other **key non-monetised benefits** by 'main affected groups' There may be additional benefits to public and private sector organisations from increased public confidence in their ability to provide goods and services.

**Key Assumptions/Sensitivities/Risks** The net present value is sensitive to deterrence benefits assumption; cost of data losses; man hours lost by public and private sector organisations; ICO assessment notices running costs; and value of working time assumptions.

Price Base Year 2008	Time Period Years 10	<b>Net Benefit Range (NPV)</b> £ 84.6m – 108.7m	<b>NET BENEFIT (NPV Best estimate)</b> £ 77.0m
-------------------------	-------------------------	--	---

What is the geographic coverage of the policy/option?		United Kingdom		
On what date will the policy be implemented?		April 2010		
Which organisation(s) will enforce the policy?		ICO/Courts		
What is the total annual cost of enforcement for these organisations?		£ 2m		
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	No	No

<b>Impact on Admin Burdens Baseline (2008 Prices)</b>				(Increase -
Increase	£ 2.5m	Decrease	£ 0	<b>Net</b> £ 2.5m

Key: **Annual costs and benefits:** (Net) Present

### 1. Scope of the Impact Assessment

- 1.1 This Impact Assessment (IA) assesses the social costs and benefits of implementing the statutory measures the Government is considering taking, through the Coroners and Justice Bill (“the Bill”), to strengthen the Information Commissioner’s power to conduct inspections and assessments under the Data Protection Act 1998 (DPA). The IA reflects discussions held with the Information Commissioner’s Office as well as consideration of debates held in the House of Commons between January and March 2009 and reports from the Joint Committee on Human Rights and the Lords Select Committee on the Constitution. The assessment follows the procedures and criteria set out in the Impact Assessment Guidance and is consistent with the HM Treasury Green Book.
- 1.2 The DPA provides the Information Commissioner’s Office (ICO) 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 is therefore proposing that we enhance the UK data protection framework by introducing assessment notices, which allow the Information Commissioner to undertake mandatory “spot-checks” on certain data controllers. These assessment notices are intended to complement the existing powers of the Information Commissioner.

#### Scope of the proposals

- 1.3 The main proposals are :
- **Formalise the powers relating to public authorities** - currently, the Information Commissioner can conduct “spot checks” of government departments using the powers he has under s51(7) of the DPA. The Bill would *formalise* and extend the power to other public authorities beyond Government Departments.
  - **New powers to regulate certain classes of private sector data controllers** – the Government proposes to extend the scope of the power so that, in addition to public authorities, other private sector data controllers may be liable for assessment notices. A combination of “blanket” and “liable by order” options are explored.

#### Organisations in the scope of the legislation

- 1.4 The main group affected by the proposal is data controllers established in the UK, including public and private sector organisations (aside from those few groups excluded by legislation). According to the Information Commissioner’s public register, there are currently 319,928 registered data controllers in the UK covering both the public and private sectors.
- 1.5 The proposals would also have an impact on the workload of the Information Commissioner’s Office. There may also be an increase in the number of appeals to the Information Tribunal and applications to the Courts for warrants under Schedule 9 to the DPA.

## Analytical Principles

- 1.6 This IA identifies as far as possible both monetised and non-monetised impacts from society's perspectives, with the aim of understanding what the net social impact to society might be from the introduction of Assessment Notices.
- 1.7 Cost benefit analysis places a strong emphasis on the monetisation of costs and benefits. However there are important aspects that cannot sensibly be monetised. These might be distributional impacts on certain groups of society or some institutional impacts, either positive (e.g. increased deterrence) or negative (e.g. costs on the justice system). Cost benefit analysis in this IA is therefore interpreted broadly, to include both monetisable and non-monetisable costs and benefits, with due weight given to those that are non-monetisable.
- 1.8 An important consideration for any cost benefit analysis is the relevant scope of the assessment. The scope of this IA is defined to include :
- Impacts that fall within the United Kingdom - that is to say we have tried to capture all the impacts that fall on UK firms and their consumers.
  - Impacts that fall on both present and future generations - in line with the HMT Green Book and IA Guidance, the appraisal assesses whether any of the options will yield a positive net social benefit to all who may be affected by it. As the Assessment Notices will continue in the distant future, we have appraised the impacts between 2010 and 2019 (10 years). A real discount rate of 3.5% is applied.

## 2. Rationale for Government Intervention

- 2.1 The conventional economic approach to Government intervention is based on efficiency or equity arguments. Government intervenes if there is a perceived failure in the way markets operate ("market failures") or it would like to correct existing institutional distortions ("government failures"). Government also intervenes for equity or fairness reasons. In this context the relevant "market" can be defined as "data handling". The public and private sectors engage in transactions with the consumers which involve the storage and handling of personal data. The question is whether this activity represents a market failure, which needs to be corrected. In economic terms, we are essentially asking whether data handling imposes wider costs on society that are *not borne* by businesses or the public sector. More importantly, we are asking whether these costs are greater than the benefits to society in general of data handling.
- 2.2 There are good reasons to believe that the storage of personal data does indeed impose wider costs on society. The storage of personal data involves handling of personal data in large quantities that is sometimes lost or stolen from data controllers and used for purposes not intended by the original owners. When a person shares personal data with a public body due to a public obligation to provide that personal data, but it is later lost and possibly used for fraud and other criminal activities, it is likely that many people who are victims would suffer loss.

- 2.3 Economists would say that an *externality* is present. Poor data handling by public and private sector organisations leads to subsequent data loss that potentially imposes costs on individuals.
- 2.4 These costs are mitigated, to some degree, if individuals are fully informed about which organisations are poor at storing personal data and are able to opt out of engaging with them. However, in practice this is not always possible for two reasons. First, individuals often do not have sufficient information on the data storage capacity of organisations they deal with and hence may not be informed enough to credibly identify the sources of the data breaches (they experience the data losses but are not always fully aware of its source). Secondly, in many cases, especially with public sector organisations, individuals are compelled to provide personal data and therefore are not in a position to withdraw cooperation even in the face of data losses.
- 2.5 This consideration suggests that the external costs of data storage could be significantly reduced through an effective and efficient regulatory system that improves information available to consumers and protects their interests. The proposals in this IA support an inspection regime that seeks to correct these failures through a system of inspections and assessments. Government aims to ensure the Information Commissioner has sufficient powers to undertake inspections of data controllers, and to ensure compliance with the data protection principles. Increased *external scrutiny* would provide a strong incentive for data controllers to comply with their obligations under DPA. In particular, the introduction of assessment notices is another step to improve the deterrent effect and correct the external costs associated with information losses.
- 2.6 The DPA transposes EU Directive 95/46/EC. The current proposal is in line with the EU requirement set out in Article 28 of the Directive that the Information Commissioner shall “in particular be endowed with investigative powers, such as powers of access to data forming the subject-matter of processing operations and powers to collect all the information necessary for the performance of [his] supervisory duties”. As the Government has provided investigative powers in the form of information notices, provision for assessment notices for Government departments, the wider public sector and any other category of data controller can be seen as going beyond minimum EU requirements. However, this is mitigated by the fact that the new assessment tool is in line with Macrory regulatory principles. In addition, consultation will be carried out before any category of data controller is designated. In addition each designation will need to be considered and approved by both Houses of Parliament.

### 3. Cost Benefit Analysis

- 3.1 This section sets out some potential costs and benefits of implementing the proposed legislation of enhancing the Information Commissioner’s power to conduct inspections and assessments under the DPA.

## BASE CASE

### Description

- 3.2 The Impact Assessment and HMT Treasury Green Guidance require that all options are assessed relative to a common 'base case' over the appropriate appraisal period of the relevant 'do-something' options. The base case would see the maintenance of the current powers of the Information Commissioner. These powers include:
- The DPA provides powers to the Information Commissioner to serve data controllers with *information notices* (requiring information to be provided as specified), *enforcement notices* (requiring a data controller to take steps to comply with the data protection principles) and provide that he may also apply to the courts for a warrant for *search and seizure*. These will remain in place under the proposals.
  - The DPA also places a duty on the Information Commissioner to promote good practice and, under s51(7), he may carry out a '*good practice assessment*' on any data controller, whether in the public or private sector, subject to their consent. The Prime Minister has said that the Commissioner may undertake these assessments on central government departments at any time. This is the basis for a current regime of "spot checks" on Whitehall departments, but this does not extend either to the wider public sector or to the private sector.
  - The Criminal Justice and Immigration Act (2008), when commenced by secondary legislation, will enable the Information Commissioner to issue *Civil Monetary Penalties* for serious, deliberate or reckless breaches of the data protection principles of a kind likely to cause substantial harm or substantial distress.
- 3.3 Certain drivers are likely to change over time that may amplify the profile of costs and benefits within the base case over time relative to the *current year*. Understanding the profile of these drivers over time is crucial before formal assessment is made of the *incremental impacts* of introducing do-something options.

### Data Controllers

- 3.4 In 2009, there were about 319,000 data controllers operating in the United Kingdom, and this is expected to increase over time. **Table 1** presents the current trend in the number of data handlers. More data handlers over time would increase the risk of data breaches over time.

<b>Year</b>	<b>Registered Firms</b>
Mar-2005	259,296
Mar-2006	271,722
Mar-2007	287,115
Mar-2008	304,551
Mar-2009	317,165
Jun-2009	319,928

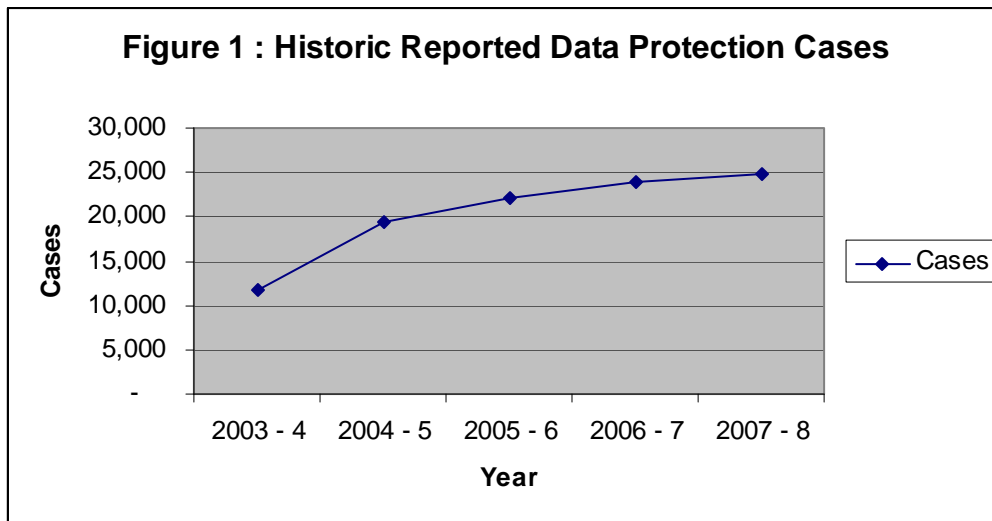
*Source : Information Commissioner's Office*

## Personal Data Storage

3.5 As public and private sector firms rely more and more on technology to handle increasing amounts of personal data to provide services and goods, it is likely that the risk of data breaches in all sectors will increase proportionately. There are also indications that in times of economic downturn instances of malicious data theft and hacking increase, including action by ex-staff who have suffered redundancies<sup>1</sup>.

## Data Protection Cases

3.6 The increasing number of data handlers and data storage has correlated with increasing levels of data protection cases handled. **Figure 1** shows the level of complaints or enquiries made to the ICO since 2003.



3.7 However, it should be noted that not all these Data Protection Cases are associated with information breaches or can be classified as “complaints”. Some were simply requests for advice and guidance.

3.8 In terms of information breaches, figures collected by the Information Commissioner's Office show that from November 2007 to April 2009, the private sector reported 143 breaches of a total of 471 reported to the Commissioner. More breaches may have occurred, but there is no obligation to report breaches under UK law. In addition, the ICO's Annual Report 2008 reveals that over 50% of complaints received were made in relation to the private sector<sup>2</sup> and 6 of 9 formal undertakings to the ICO not to breach the DPA in that year were made by private sector organisations<sup>3</sup>.

<sup>1</sup> 'Unsecured Economies: Protecting Vital Information' (McAfee Report, January 2009) p9

<sup>2</sup> Information Commissioner's Office Annual Report 2007-08, p31

<sup>3</sup> Ibid, p35

## OPTION 1

### Description

- 3.9 **Allow the Information Commissioner to undertake mandatory assessments of central government departments and such other public authorities that are designated as liable by Order.** The practical implications would be as follows:
- *Formalise* the use of assessment notices for Central Government Departments.
  - Introduce *new mandatory assessment for all public authorities* (throughout this Impact Assessment the terms “public authorities” and “public sector” include bodies exercising functions of a public nature and carrying out the functions of a public authority under contract). This represents a new mandatory requirement for non-central government departments, if that authority is designated as liable for assessment notices by Order;
  - There would be a right of appeal for the data controller to the *Information Tribunal* against an assessment notice.
  - The Information Commissioner will *not be able to serve a civil monetary penalty* on the data controller as a direct result of the findings of an assessment;
  - No assessment notices would be issued to private sector data controllers. For the private sector (other than those that could be designated as public authorities), the arrangement of negotiated good practice assessments would continue.

### Costs of Option 1

- 3.10 Option 1 would impose direct and indirect costs on society relative to the ‘base case’ scenario. Direct costs are defined as first round impacts that would be borne directly by the Information Commissioner. Indirect costs are second round impacts that would be borne by businesses, their customers and the justice system.

#### First Round Costs

- 3.11 The main direct costs associated with Option 1 are the administration costs on the Information Commissioner’s Office and the resource burden on the affected public authorities.

#### *Administrative Costs*

- 3.12 The overall cost of setting up the new regulatory regime is estimated at a one off cost of £2.5m, with annual costs of around £4.5m. These costs include, but are not limited to assessment notices, and include hiring staff and providing training. We estimate the *additional* costs of assessment notices would be around £2m annually or around net present cost of £17.2m over the next 10 years.

- 3.13 There are also direct costs on public authorities emanating from the formalisation of the assessment notices process on Central Government Departments and possible assessment notices on other authorities designated as liable by order. The estimation of resource burdens is based on the following assumptions :
- i. *Number of additional assessment notices*: It is difficult to predict with certainty how many assessment notices would be undertaken annually under Option 1. We have assumed that around 25 assessment notices would take place. As there is no current statutory obligation on Government to undertake assessment notices, we have assumed Option 1 would impose *additional burden* in the long term on both central government departments and other public authorities designated as liable by order.
  - ii. *Resource costs per assessment notice*: In many cases the costs to the data controller will be negligible, involving providing information to the ICO in order to establish compliance or otherwise with the data protection principles. In more involved cases, staff may be diverted from their core duties to provide the ICO with information. We have estimated the resource cost to organisation per assessment notice based on data from a typical “good practice assessment”. A “central case” assumption of around 70 man-hours for each assessment is used. Based on the in-work values of time published by the Department for Transport, we estimate a typical man-hour lost in 2010 would be around £39.48 (2008 prices). This equates to around £2,764 per assessment notice in 2010.
- 3.14 Under Option 1, we assume that 25 assessment notices would be served annually. This would represent an annual burden on the public sector of around £69,000. Over 2010 – 2019, this would equate to a net present value (discounted) of around £628,000 for the “central case”.
- 3.15 Due to the inherent uncertainty over the number of man-hours, we have considered both low and high scenarios. The advice from the ICO suggests a range from 7 hours for small assessment to 73 for larger assessments. The expectation is that assessment notices will be targeted predominantly at larger organisations, hence the assumption of 70 hours in the central case, which is closer to the 73 hours suggested by the ICO. We have applied a +/-10% assessment around this figure, to give a low and high sensitivity range of 63 hours – 77 hours. Based on this range, the additional resource burdens would range between £564,745 and £690,244.

## Second Round Costs

- 3.16 The main indirect costs associated with Option 1 would depend on the extent to which the terms of assessment notices were accepted. There may be an impact on the work of the Information Tribunal as a result of appeals made further to assessment notices being served. However, the chances of a public authority appealing an assessment notice are low, given the bad publicity which would ensue. It is more likely that, in the unlikely event of a dispute over the terms of an assessment notice, the authority would come to an informal agreement with the ICO.

## Benefits of Option 1

3.17 Option 1 would impose direct and indirect benefits on society relative to the 'base case' scenario.

### First Round Benefits

- 3.18 The main direct benefits associated with Option 1 are greater protection of personal data held by public sector organisations. This would be two-fold:
- Swifter correction of data mishandling: the ICO will be able to identify sooner examples of bad practice within the public sector and will subsequently be able to require those public sector data controllers to take steps to rectify these practices. The personal data of these citizens will therefore enjoy greater protection.
  - Deterrent effect: In so far as assessment notices will reveal poor practices to the public, this would have reputational consequences for the relevant organisations. It's therefore possible that mandatory assessment notices may provide a significant deterrent effect. However, the extent to which this might be the case would largely depend on the regulatory regime as a whole.
  - Improved confidence for the public: although the extent to which individuals choose whether to provide personal data to a public sector organisation is limited, there are still areas where such choices exist e.g. provision of benefits, travel information etc. Assessment notices will provide additional assurance about how public sector data controllers handle their personal data.
- 3.19 It is difficult to estimate precisely how many data mishandling cases may be prevented by a more effective regime supported by assessment notices, within the context of Option 1. In addition, there is no definitive assessment of how much mishandling of data costs organisations. Research carried out by the Ponemon Institute in 2008 suggested that each data breach cost an organisation an average of £1.7 million. For the purposes of this Impact Assessment, we will rely on the more conservative 2007 estimate of a £1.4m cost per data breach<sup>4</sup>. We use this figure with the caveat that it is subject to considerable uncertainty. The ICO has announced its intention to undertake research to quantify the risks of holding information, and place a monetary value on information as an asset<sup>5</sup>.
- 3.20 The "central case" assumption is that assessment notices would contribute to at least a reduction of two public sector data mishandling cases annually, leading to a net present benefit of around £24.2m. Due to the inherent uncertainty around this result, we have considered the possibility of 1 - 3 range of public sector data mishandling cases prevented. This produces a range of £12.1m - £36.3m.

---

<sup>4</sup> 2008 Annual Study: Cost of a data breach, Ponemon Institute (February 2009), pp11-12

<sup>5</sup> ICO press release 18 June 2009 'Putting a price on privacy protection'

## Second Round Benefits

3.21 The main indirect benefits associated with Option 1 are to those data controllers in the public sector that rely on personal data given voluntarily to provide services, as the higher level of scrutiny should be accompanied by a greater degree of confidence in the public sector in its handling of personal data. This will allow those public sector data controllers to provide better services, in turn providing greater benefits to citizens.

### Net Impact of Option 1

3.22 Option 1 would generate a net positive impact of around £10m. This is based on Option 1 supporting an inspection regime that prevents at least two data case of mishandling annually and each assessment notice imposing 70 man hours on an average public sector organisation. Both of these assumptions are subject to significant uncertainty. **Table 2** provides the central and sensitivity tests result.

<b>Table 2 : Option 1 Costs and Benefits (£m)</b>			
	<b>Costs</b>	<b>Benefits</b>	<b>Net Present Value</b>
<b>Central Case</b>	17.9	24.2	6.3
<b>Test 1: 63 man-hours per assessment</b>	17.8	24.2	6.4
<b>Test 2: 77 man-hours per assessment</b>	17.9	24.2	6.3
<b>Test 3: 1 case deterred / prevented by assessments</b>	17.9	12.1	-5.8
<b>Test 4: 3 cases deterred / prevented by assessments</b>	17.9	36.3	18.4

## OPTION 2

### Description

3.23 **Allow the ICO to undertake mandatory assessments of central government departments, public authorities as designated by order, and all private data controllers who are members of descriptions that are designated as liable by Order (preferred option)** The practical implications would be as follows:

- *Formalise* the use of assessment notices for Central Government Departments;
- Introduce *new mandatory assessments for public and private sector bodies*, this represents a new mandatory requirement for all organisations, if the authority is designated or the description to which that organisation belongs is designated as liable for assessment notices by Order;
- There would be a right of appeal for the data controller to the Information Tribunal against an assessment notice;
- If a data controller fails to comply with the terms of an assessment notice, the Commissioner may cite this non-compliance as grounds for obtaining a search warrant under Schedule 9 to the DPA;
- The Information Commissioner will not be able to serve a civil monetary penalty on the data controller as a direct result of the findings of an assessment;
- The ICO has stated its view that its “risk-based approach is in line with the principles of regulatory good practice”.

## Costs of Option 2

- 3.24 The main direct costs associated with Option 2 are the administration costs on the Information Commissioner's Office and the resource burden on the affected public and private sector organisations.

### First Round Costs

- 3.25 The first round costs for Option 2 are the same as for Option 1. These are estimated at £17.9m between 2010 and 2019 for public sector organisations. However, there are additional resource burdens imposed on the private sector. We have assumed that private sector organisations would face an additional 25 assessments per year, translating to an additional £0.68m worth of costs between 2010 and 2019. The costs to the Information Commissioner's Office are assumed to be the same, as it will be increasing its audit capability in other ways with the resources available. The full direct costs associated with Option 2 are therefore estimated at £18.58m in the "central case".
- 3.26 Additional burdens based on a +/-10% range around the 70 hours of resource burdens assumed in the central case, provides full direct costs within the range of £18.3m - £18.6m.

### Second Round Costs

- 3.27 As with Option 1, Option 2 may lead to some potential impact on the work of the Information Tribunal as a result of appeals made further to assessment notices being served. However, the impact of Option 2 may be more significant because the private sector data controllers may be more willing to appeal an assessment notice, particularly if they believe its terms will disrupt their business severely. There may also be a small impact on the work of the Courts, as the Commissioner applies for Schedule 9 warrants in those cases where a data controller has failed to comply with an assessment notice.

## Benefits of Option 2

- 3.28 Option 2 would impose direct and indirect benefits on society relative to the 'base case' scenario.

### First Round Benefits

- 3.29 Same as Option 1. There would be direct benefits to society in terms of swifter correction of data mishandling; an increased deterrent effect of the ICO inspection regime; and greater information to the public. However, under Option 2 the deterrent effect is assumed to be greater due to the wider application of assessment notices. We have assumed that Option 2 would support the prevention of at least four data mishandling cases annually under the "central case". This could potentially lead to benefits of up to £48.3m between the period 2010 and 2019.
- 3.30 In line with Option 1, we have assumed a sensitivity test around these figures of +/-1 prevented cases. This produces a sensitivity range for potential "prevention benefits" under Option 2 between £36.3m - £60.4m.

## Second Round Benefits

3.31 Same as Option 1. There may be additional benefits to public sector organisations from increased public confidence in their ability to provide services. Additionally, an assessment which produces a positive result (a “clean bill of health”), if announced publicly, may attract consumers to a private sector data controller and encourage them to provide personal data. This in turn will allow those data controllers to provide better goods and services, providing benefits to the consumer.

## Net Impact of Option 2

3.32 Option 2 would generate a net positive impact of around £29.8m. This is based on Option 2 supporting an inspection regime that prevents at least four data cases of mishandling annually and each assessment notice imposing a burden of 70 man hours on an average organisation under the “central case”. Both of these assumptions are subject to significant uncertainty. **Table 3** provides the central and sensitivity tests result.

Table 3 : Option 2 Costs and Benefits (£m)			
	Costs	Benefits	Net Present Value
Central Case	18.5	48.3	29.8
Test 1: 63 man-hours per assessment	18.3	48.3	30.0
Test 2: 77 man-hours per assessment	18.6	48.3	29.7
Test 3: 3 cases deterred / prevented by assessments	18.5	36.3	17.8
Test 4: 5 cases deterred / prevented by assessments	18.5	60.4	41.9

## OPTION 3

### Description

3.33 **Allow the Information Commissioner to carry out mandatory assessments of all data controllers.** The practical implications would be as follows:

- *Formalise* the use of assessment notices for Central Government Departments.
- Introduce *new mandatory assessment* for all data controllers without prior notice;
- There would be a right of appeal for the data controller to the *Information Tribunal* against an assessment notice;
- If a data controller fails to comply with the terms of an assessment notice, the Commissioner may cite this non-compliance as grounds for obtaining a search warrant under Schedule 9 to the DPA;
- Information Commissioner will *not be able to serve a civil monetary penalty* on the data controller as a direct result of the findings of an assessment.

## Costs of Option 3

- 3.34 The main direct costs associated with Option 3 are the administration costs on the Information Commissioner's Office and the resource burden on the affected public and private sector organisations.

### First Round Costs

- 3.35 The first round costs for Option 3 are the same as for Option 2. These are estimated at £18.58m based on 50 assessment notices, split equally between the private and public sectors. We have estimated that this measure would result in an additional 50 more assessment notices for the private sector over and above the 25 assumed under Option 2, bringing the overall total of assessment notices (for both public and private sectors) above the base to around 100. The full direct costs associated with Option 3 are therefore estimated at £19.7m.
- 3.36 Additional sensitivity tests based on a +/-10% range around the 70 hours of resource burdens assumed in the central cases, provides full direct costs within the range of £19.5m - £20.0m.

### Second Round Costs

- 3.37** Similar to Options 1 and 2, Option 3 may lead to some potential impact on the work of the Information Tribunal as a result of appeals made further to assessment notices being served. However, the impact of Option 3 may be more significant because the mandatory nature of Option 3 would increase the number of private sector data controllers affected and the likelihood of appealing the assessment notice, particularly if they believe its terms will disrupt their business severely. There may also be a larger impact on the work of the Courts, as the Commissioner applies for Schedule 9 warrants in those cases where a data controller has failed to comply with an assessment notice, relative to Options 1 and 2.

## Benefits of Option 3

- 3.38 Option 3 would impose direct and indirect benefits on society relative to the 'base case' scenario.

### First Round Benefits

- 3.39 The main direct benefits for Option 3 are the same as those for option 2 (above). There is a small administrative benefit in not having to designate data controllers by Order to carry out an assessment.
- 3.40 Same as Options 1 and 2. There would be direct benefits to society in terms of swifter correction of data mishandling; increased deterrent effect of the ICO inspection regime; and greater information to the public. However, under Option 3 the deterrent effect is assumed to be greater due to the wider application of assessment notices and the greater powers to the ICO. We have assumed that Option 3 would support the prevention of at least 8 data mishandling cases under the "central case". This could lead to benefits of around £96.7m between the period 2010 and 2019.
- 3.41 In line with Option 1, we have assumed a sensitivity test around these figures of +/-1 prevented cases. This produces a sensitivity range for potential "prevention benefits" under Option 3 ranging between £84.6m - £108.7m.

## Second Round Benefits

3.42 Same as Options 1 and 2. There may be additional benefits to public sector organisations from increased public confidence in their ability to provide a service, especially for voluntarily services. Additionally, an assessment which produces a positive result (a “clean bill of health”) may attract consumers to a private sector data controller and encourage them to provide personal data. This in turn will allow those data controllers to provide better goods and services, providing benefits to the consumer.

### Net Impact of Option 3

3.43 Option 3 would generate a net positive impact of around £77m. This is based on Option 3 supporting an inspection regime that prevents at least eight cases of data mishandling annually and each assessment notice imposing 70 man hours on an average organisation under the “central case”. Both of these assumptions are subject to significant uncertainty. **Table 4** provides the central and sensitivity tests result.

<b>Table 4 : Option 3 Costs and Benefits (£m)</b>			
	<b>Costs</b>	<b>Benefits</b>	<b>Net Present Value</b>
<b>Central Case</b>	19.7	96.7	77.0
<b>Test 1: 63 man-hours per assessment</b>	19.5	96.7	77.2
<b>Test 2: 77 man-hours per assessment</b>	20.0	96.7	76.7
<b>Test 3: 7 cases deterred / prevented by assessments</b>	19.7	84.6	64.9
<b>Test 4: 9 cases deterred / prevented by assessments</b>	19.7	108.7	89.0

## Summary of Options Analysis

3.44 **Table 5** presents a summary of the quantified costs and benefits based on the assumptions discussed above. The net economic benefits range from £11.0m to £83.7m depending on the nature of the option and deterrence assumptions.

<b>Table 5 : Summary of Options (£m)</b>			
	<b>Costs</b>	<b>Benefits</b>	<b>Net Present Value</b>
<b>Option 1</b>	17.9	28.9	11.0
<b>Option 2</b>	18.6	56.8	38.2
<b>Option 3</b>	19.9	103.6	83.7

3.45 We have also assessed the non-monetised impacts of the three options. In general all options would lead to monetised costs in terms of impact on the Information Tribunal and justice system. However, in so far as Option 3 provides greater powers to the ICO, we would expect it to impose greater costs on the Information Tribunal and the justice system, especially with respect to applications for Schedule 9 warrants.

3.46 The non-monetised benefits relate to increased data security within public and private sector organisations from increased public confidence in their ability to provide goods and services. These benefits are likely to be larger under Options 2 and 3 where some degree of deterrence is introduced for private sector data handlers.

- 3.47 However, despite the benefits in terms of greater compliance with the DPA and subsequent data breach preventions offered by Option 3, we are sensitive to the concerns that have been expressed about a blanket extension of this power to all data controllers. We wish to see a focussed assessment mechanism, with parliamentary oversight and a review mechanism, in line with good regulatory practice. We therefore favour Option 2 over the more blanket extension to the private sector offered by Option 3.

#### 4. Enforcement and Implementation

- 4.1 Options (1), (2) and (3) will come with a right of appeal for the data controller to the Information Tribunal. Under options (2) and (3), if a data controller fails to comply (or partially fails to comply) with the requirements of an assessment notice, this will be grounds for the Information Commissioner to apply to the court for a warrant for entry to and search of a data controllers' premises under Schedule 9 to the DPA. The ICO will also be obliged under statute to issue (and review when necessary) a Code of Practice on assessment notices, both the original and revisions of which will be subject to approval by the Secretary of State.

#### 5. Competition Assessment

- 5.1 A preliminary competition filter was undertaken and is set out **Annex A**. This revealed that there are no impacts on competition, therefore a full assessment was not necessary.

#### 6. Small Firms Impact Assessment

- 6.1 It is impossible to know how small firms will be affected by the new power, without an indication of which classes of data controller the ICO would propose to designate as liable for assessment notices. However, as mentioned above, the ICO has indicated that they would be more likely to serve assessment notices on larger data controllers, as these hold more extensive collections of personal data, and more sensitive personal data. It is proposed that such an assessment is carried out as part of the process for so designating a description on a case-by-case basis.

#### 7. Legal Aid and Justice Impact Test

- 7.1 The impact on the justice system has been assessed as part of the options analysis (see **Section 2**).

#### 8. Race / Disability / Gender Equality

- 8.1 A preliminary EIA filter was undertaken and is set out **Annex B**. None of the options considered have any impact on Race, Disability or Gender of individuals.

## **9. Human Rights**

- 9.1 The proposals are compliant with the Human Rights Act 1998.

## **10. Environment/Rural/Health**

- 10.1 There are no anticipated environmental impacts associated with the options presented, nor are any significant rural or health issues anticipated.

## 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.**

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

## COMPETITION ASSESSMENT

### **Would the proposals:**

#### **Directly limit the number or range of suppliers?**

No. Assessments carried out further to an assessment notice would only reveal compliance or otherwise with the data protection principles, with which the data controller should be complying under the Data Protection Act 1998 (DPA).

#### **Indirectly limit the number or range of suppliers?**

No. As above, assessments carried out further to an assessment notice would only reveal compliance or otherwise with the data protection principles. The Information Commissioner cannot serve a data controller with a civil monetary penalty as a result of the findings of an assessment. However, he can subsequently serve an enforcement notice on the data controller, requiring them to take steps to comply with the data protection principles. Failure to comply with an enforcement notice is an offence.

#### **Limit the ability of suppliers to compete?**

No. An assessment carried out further to an assessment notice would not be so detailed as to impede a data controllers' ability to compete. If a data controller felt this would happen, it is open to them to appeal the assessment notice to the Information Tribunal.

#### **Reduce suppliers' incentives to compete vigorously?**

No. The possibility of a mandatory assessment regime would rather provide an incentive for businesses to maintain high standards in their data processing, given the bad publicity that would ensue from a negative assessment report from the Information Commissioner.

As the impacts on competition are negligible no formal Impact Assessment has been undertaken.

## Equality Impact Assessment Initial Screening – Relevance to Equality Duties

The EIA should be used to identify likely impacts on:

- Disability
- Gender (including gender identity)
- Race
- Age
- Caring responsibilities (usually only for HR policies and change management processes such as back offices)
- Religion and belief
- Sexual orientation

1. Name of the proposed new or changed legislation, policy, strategy, project or service being assessed

Allowing the Information Commissioner to carry out mandatory assessments of central government departments and such data controllers (whether in the public or private sector) as are designated as liable by Order.

2. Individual officer(s) & Unit responsible for completing the Equality Impact Assessment:

Ollie Simpson, Information Policy Division

3. What is the main aim or purpose of the proposed new or changed legislation, policy, strategy, project or service and what are the intended outcomes?

### Aims/objectives

We are proposing to strengthen the Information Commissioner's powers under the Data Protection Act 1998 (DPA) to conduct assessments of those private sector organisations designated as liable by order, further to consideration of:

- the volume and nature of the personal data they handle;
- the damage or distress that could be caused by a breach of the data protection principles by that class,

### Outcomes

Raised awareness of and compliance with the data protection principles in the private sector.

4. What existing sources of information will you use to help you identify the likely equality on different groups of people?

Comparative existing policies: for example spot checks of Government departments and good practice assessments carried out under s51(7) of the DPA.

5. Are there gaps in information that make it difficult or impossible to form an opinion on how your proposals might affect different groups of people. If so what are the gaps in the information and how and when do you plan to collect additional information?

We do not know for certain which classes of data controller the Information Commissioner will recommend for designation as liable for assessment notices (however, he will be obliged to have regard to the nature and quantity of the personal data being handled by that class of data controllers, and the damage or distress that would be caused by a contravention of the data protection principles). The Secretary of State would need to consider the same factors in deciding whether to make an order on the basis of the ICO's recommendation. An impact assessment (including consideration of an Equality Impact Assessment) would be prepared for each recommendation the Secretary of State was minded to take forward, and he would be obliged to consult representatives of those affected

Once a class or category of data controller is designated as liable, we do not know on which data controllers the ICO will choose to serve an assessment notice, nor the extent of each assessment. However, on the basis of information supplied by the ICO, we can say that smaller assessments will last 1-2 days, involving fewer of the data controller's staff, and larger assessments will last 3-4 days, involving more of the data controller's resources. This represents a burden of between 7 and 70 man hours per assessment.

We will seek information from the ICO about the man hours involved in assessments carried out further to assessment notices, when these begin to take place in order to understand better the impact on data controllers.

6. Having analysed the initial and additional sources of information including feedback from consultation, is there any evidence that the proposed changes will have a **positive impact** on any of these different groups of people and/or promote equality of opportunity?

Please provide details of who benefits from the positive impacts and the evidence and analysis used to identify them.

Improved compliance with the Data Protection Act 1998 would help to ensure that decisions surrounding suitability for (for example) employment and credit were based on accurate and up to date information, which would benefit many groups. Accurate and up to date information would also lead to the more efficient allocation and delivery of public services and benefits.

7. Is there any feedback or evidence that additional work could be done to promote equality of opportunity?

If the answer is yes, please provide details of whether or not you plan to undertake this work. If not, please say why.

No

8. Is there any evidence that proposed changes will have **an adverse equality impact** on any of these different groups of people?

Please provide details of who the proposals affect, what the adverse impacts are and the evidence and analysis used to identify them.

n/a

9. Is there any evidence that the proposed changes have **no equality impacts**?

Please provide details of the evidence and analysis used to reach the conclusion that the proposed changes have no impact on any of these different groups of people.

The Information Commissioner intends to carry out assessments on those data controllers designated as liable by order, further to consideration of:

- the volume and nature of the personal data they handle;
- the damage or distress that could be caused by a breach of the data protection principles by that class of data controllers.

According to the KPMG Data Loss Barometer (published September 2008), those sectors within the private sector which are responsible for most data losses are financial services, consumer markets, and information, communications and entertainment sectors. Losses from consumer markets affect the greatest number of people.

10. Is a full Equality Impact Assessment Required?  
(If no, please explain why not)

No

There is no evidence put forward to suggest that the data breach patterns identified in the KPMG report, or any other research, break down along grounds of disability, gender, race etc

11. If a full EIA is not required, you are legally required to monitor and review the proposed changes after implementation to check they work as planned and to screen for unexpected equality impacts. Please provide details of how you will monitor evaluate or review your proposals and when the review will take place.

A full impact assessment (including an Equality Impact Assessment) would be prepared for each ICO recommendation the Secretary of State was minded to take forward.

This general policy would be reviewed in 5 – 10 years. An evaluation strategy would be prepared to help collect data for monitoring purposes.

## 12. Name of Senior Manager and date approved

We are proposing to strengthen the Information Commissioner's powers via the Coroners and Justice Bill to conduct assessments of those private sector organisations designated as liable by order, further to consideration of:

- the volume and nature of the personal data they handle;
- the damage or distress that could be caused by a breach of the data protection principles by that class.

There is no evidence from emerging studies and reports that this will have a particular impact on equality in the areas of disability, gender (including gender identity), race, age, caring responsibilities, religion and belief or sexual orientation. However, a full impact assessment (including consideration of the impact on equality) would be prepared for each ICO recommendation the Secretary of State was minded to take forward.

Name (must be grade 5 or above): Belinda Lewis

Department: Information Policy Division, Information Directorate, Ministry of Justice

Date: 09/11/2009

Note: If a full EIA is required hold on to the initial screening and when the full EIA is completed send the initial and full screening together.  
**If a full EIA is not required send the initial screening by email to the Equality, Diversity and Human Rights Division for publication**

