EXPLANATORY MEMORANDUM TO

THE DATA PROTECTION (MONETARY PENALTIES) (MAXIMUM PENALTY AND NOTICES) REGULATIONS 2010

2010 No. 31

AND

THE DATA PROTECTION (MONETARY PENALTIES) ORDER 2010

2010 No. [DRAFT]

1. This explanatory memorandum has been prepared by the Ministry of Justice and is laid before Parliament by Command of Her Majesty.

2. Purpose of the instrument

2.1 The first, the Data Protection (Monetary Penalties) (Maximum Penalty and Notices) Regulations 2010, prescribes the maximum amount of a monetary penalty. It also sets out the minimum details to be contained in a notice of intent, and in a monetary penalty notice. This Statutory Instrument is subject to the negative resolution process.

2.2 The second, the Data Protection (Monetary Penalties) Order 2010 sets out procedural details of the issue of a monetary penalty notice following a notice of intent. It also contains details of when enforcement action can be taken, and the power to cancel or vary a monetary penalty notice issued by the Information Commissioner, as well as details of appeal rights of data controllers. This Statutory Instrument is subject to approval by resolution of each House of Parliament.

2.3 Taken together, these instruments create a framework for the Information Commissioner to serve a monetary penalty notice on a data controller if he is satisfied there has been both a serious contravention by the data controller of the data protection principles and that the contravention was of a kind likely to cause substantial damage or distress. Such contraventions must be either deliberate or something which the data controller knew would occur (or ought to have known) and of a kind likely to cause substantial damage or substantial distress, but in respect of which he failed to take reasonable steps to prevent. Both instruments will come into force together.

3. Matters of special interest to the Joint Committee on Statutory Instruments

3.1 None.

4. Legislative Context

4.1 The Data Protection Act (DPA) was amended by section 144 of the Criminal Justice and Immigration Act 2008 to provide the Information Commissioner's Office (ICO) with a power to impose a civil monetary penalty on data controllers.

4.2 The Information Commissioner may impose a civil monetary penalty when the following criteria have been satisfied –

(a) there has been a serious contravention of section 4(4) of the DPA by the data controller,

(b) the contravention was of a kind likely to cause substantial damage or substantial distress and,

(c) either the contravention was deliberate, or the data controller knew or ought to have known that there was a risk that the contravention would occur, and that such a contravention would be of a kind likely to cause substantial damage or substantial distress, but failed to take reasonable steps to prevent the contravention.

4.3 These two instruments provide further detail on the process, procedures and time limits etcetera of sections 55A – S55E of the DPA, which will be brought into force at the same time as these sections.

5. Territorial Extent and Application

5.1 These instruments apply to the United Kingdom.

6. European Convention on Human Rights

6.1 Michael Wills MP (Minister of State) has made the following statement regarding compatibility with the European Convention on Human Rights:

"In my view the provisions of the Data Protection (Monetary Penalties) Order 2010 are compatible with the European Convention on Human Rights."

6.2 As the Data Protection (Monetary Penalties) (Maximum Penalty and Notices) Regulations 2010 is subject to negative resolution procedure and does not amend primary legislation, no statement is required.

7. Policy background

7.1 Following the significant losses of personal data in 2007, a number of requests from members of the House of Lords, House of Commons and the public were made to introduce a criminal offence for reckless or repeated security breaches of personal data. The Government considered that a criminal offence would be a disproportionately heavy-handed penalty and an inadequate deterrent to regulatory non-compliance. Additionally, criminal proceedings could result in a costly and time-consuming process for data controllers and the ICO. The Information Commissioner's Office subsequently agreed with the Ministry of Justice that a civil monetary penalty would be an appropriate alternative. This was supported by Parliament during the passage of the Criminal Justice and Immigration Bill in 2008.

7.2 Financial penalties for non compliance would provide a powerful deterrent for data controllers who may otherwise ignore their responsibilities under the DPA. It will also encourage data controllers to approach the ICO when they have concerns about data protection matters.

7.3 There has been widespread support for additional powers for the ICO. Mark Walport and Richard Thomas were asked in 2007 to undertake a review of the framework for the use of personal information in the public and private sectors. After extensive consultation, they published the "Data Sharing Review Report" report in July 2008 which called for "significant improvement in the personal and organisation culture of those who collect, manage and share personal data", facilitated by a strong regulator with robust powers and sanctions.

7.4 The majority view among respondents to the Data Sharing Review, and in particular members of the public, was that "*the Data Protection Act should include stronger penalties and sanctions, and that the Information Commissioner should be given increased powers and*

resources to carry out his duties more effectively". There was wide support for the ICO's powers to be more akin to those of the Financial Services Authority (FSA), or the Health and Safety Executive; others argued for custodial sentences for some breaches. The FSA itself complained of the inequity of financial firms being penalised for their errors, when other organisations "*which may handle huge quantities of personal information, fall outside the regulatory regime*".

7.5 Most data controllers comply with the data protection principles, which taken together ensure that data processing is conducted in a fair and lawful manner. However since misuse of even small amounts of personal data can have serious consequences, it is important to minimise non-compliance with the data protection principles as much as possible. It is for this reason that Government believes it is necessary to give the ICO the power to impose civil monetary penalties on those data controllers who commit a serious contravention of the data protection principles, as described in section 55A of the DPA.

8. Consultation outcome

8.1 On 9 November 2009 the Government published its consultation paper entitled "Civil Monetary Penalties, Setting the maximum penalty", which set out the proposal to set the maximum penalty for Civil Monetary Penalties at £500,000. The consultation paper sought views from data controllers on the level of the proposed penalty, but responses to the consultation were welcome from anyone with an interest. The consultation period closed on 21 December 2009. Over 70 organisations were sent a copy of the consultation paper, ranging from businesses, government departments and consumer groups. The consultation paper was also placed on the website of the Ministry of Justice.

8.2 During the same period, the ICO consulted on its draft guidance, which deals with the circumstances in which the Commissioner would consider it appropriate to issue a monetary penalty notice and how he will determine the amount of the monetary penalty. The guidance will also detail other considerations that will be taken into account, such as the sector (for example whether the data controller is a voluntary organisation), the size, financial and other resources of the data controller.

8.3. MoJ received a total of 52 responses, which came from a wide range of data controllers, including individuals, financial companies, legal bodies, local government and large businesses. The ICO responded favourably to the consultation.

8.4 The majority of respondents (53%) supported the proposal, and believed this to be a fair and proportionate approach. Although 32% were against a £500,000 maximum penalty, they were not united in the dissent; 15% thought the fixed maximum penalty was too low while 17% of responses thought it was too high.

9. Guidance

9.1 The Ministry of Justice and Information Commissioner will publicise the new power. Section 55C of the DPA places the Information Commissioner under a duty to prepare and issue guidance on how he proposes to exercise his functions in relation to imposing a monetary penalty and other procedural rights. Such guidance must not be issued without the approval of the Secretary of State, and must be laid before each House of Parliament. The new powers and the associated instruments will come into force on 6 April 2010. To comply with the Government's guidance on implementation periods, the ICO's guidance should be laid at least 12 weeks before commencement of the powers. The Commissioner also has a legislative duty to arrange for

publication of any guidance in such form and manner as he considers appropriate. The DPA provides for the Commissioner to alter or replace the guidance.

10. Impact

10.1 There may be some impact on business, charities and voluntary bodies if they receive a financial penalty, but this will only apply to those organisations who are failing to comply with existing legal obligations.

10.2 The estimated impact on the public sector is around £25,000 a year (with a one off implementation cost of £135,000). The ICO will have a one off cost of around £100,000, covering items such as staff training, printing, updating websites and so on. They will also incur an estimated annual cost of around £17,500, including legal investigative costs, legal staff costs etcetera. The cost of implementing civil monetary penalties will be met by the recent increase in the notification fee from £35 per year to £500 a year for those data controllers with either a turnover of £25.9M **and** 250 or more members of staff, **or,** public authorities with 250 or more members of staff. Government faces a one off cost of approximately £35,000 for implementing provisions within the Tribunals Service (appeals procedure) with annual running costs of around £7,500.

10.3 An Impact Assessment is attached to this memorandum.

11. Regulating small business

11.1 The legislation applies to small businesses.

11.2 To minimise the impact of the requirements on small firms employing up to 20 people, the ICO will take into account a number of factors, including financial resources of the data controller. Small businesses will therefore not be impacted disproportionately. All data controllers who have been issued with a notice of intent by the ICO of their intention to impose a civil monetary penalty will have the opportunity to provide the ICO with representations regarding the specific circumstances surrounding the alleged breach, as well as the financial impact of any proposed penalty. After a civil monetary penalty has been served there is a right of appeal to the Information Tribunal, either on the issue of a monetary penalty notice, or on the amount of the penalty.

11.3 Small businesses are not exempt from compliance with the DPA. However, their financial and other circumstances will be taken into account by the ICO.

12. Monitoring & review

12.1 The Government will work with the Information Commissioner to monitor the level of financial penalties imposed on data controllers who commit serious contraventions of the data protection principles. Any penalties imposed by the Information Commissioner will be published in his annual reports.

12.2 The policy will be reviewed within three years.

13. Contact

Please contact Ollie Simpson regarding any queries about the instruments at the Ministry of Justice Tel: 202 3334 4566 or email: Ollie.Simpson@justice.gsi.gov.uk.

Summary: Intervention & Options

Department /Agency:	Title:	
Ministry of Justice	Impact Assessment of Regulations on Civil Monetary Penalties for the Information Commissioner.	
Stage: Statutory Instrument	**Version:** 2	**Date:** 06/01/2010

Related Publications: Data Sharing Review Report (http://www.justice.gov.uk/reviews/datasharing-intro.htm); Response to the Data Sharing Review Report; Consultation Paper (http://www.justice.gov.uk/publications/response-data-sharing-review.htm); Public consultation "Civil Monetary Penalties-Setting the maximum penalty" (http://www.justice.gov.uk/consultations/civil-monetary-penalties-consultation.htm); Response to the Public consultation "Civil Monetary Penalties-Setting the maximum penalty" (http://www.justice.gov.uk)

Available to view or download at:

http://www.justice.gov.uk

Contact for enquiries: Ollie Simpson **Telephone:** 0203 334 4566

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

Following the significant losses of personal data in 2007 a number of public requests were made to introduce a criminal offence for reckless or repeated security breaches of personal data. The Information Commissioner's Office (ICO) subsequently agreed with Ministry of Justice (MoJ) that a civil monetary penalty would be an appropriate alternative.

The ICO's power to impose Civil Monetary Penalties was inserted into the Data Protection Act 1998 (DPA) through section 144 of the Criminal Justice and Immigration Act 2008.

Financial penalties for non-compliance should provide a powerful deterrent for data controllers who may otherwise ignore their responsibilities under the (DPA).

These regulations will provide the framework which, in conjunction with the guidance to be issued by the ICO, is necessary to bring into force the ICO's power to impose Civil Monetary Penalties (CMPs).

What are the policy objectives and the intended effects?

To enhance the ICO's existing powers as provided for by the DPA. This power will enable the ICO to impose financial penalties for serious contraventions of the data protection principles. This will act as a deterrent against non-compliance by data controllers, encourage data controllers to approach the ICO when they have concerns about data protection processes, and help improve public confidence in the security of personal data.

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

We have considered the following policy options:

(1) Provide for a maximum penalty.

Three amounts were considered:

1a) £50,000

1b) £500,000

1c) £2.5 million.

(2) Provide for a maximum penalty equal to 10% of the data controller's annual turnover or a maximum penalty of £500,000 if the percentage of turnover is not applicable to the data controller.

Due to the complexities of working with turnover, we considered three variants within policy option 2:

2a) Making turnover a registrable particular;

2b) Giving the ICO the power to use the £500,000 maximum penalty when establishing the data controllers annual turnover is not possible; or

2c) Creating a criminal offence - through primary legislation - for deliberately or recklessly providing the ICO with inaccurate turnover figures or not providing information at all.

Option 1(b) is the preferred option, as we believe this provides for a penalty which could act as an effective deterrent for the large majority of data controllers, and it is the most practical option in terms of enforcement.

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 3 years after implementation.

Ministerial Sign-off For Consultation Impact Assessments:

I have read the Impact Assessment and I am satisfied that (i) it represents a fair and reasonable view of the expected costs, benefits and impacts of the policy and (ii) the benefits justify the costs.

Signed by the responsible Minister:

Michael Wills

Date: 07/01/2010

Summary: Analysis & Evidence

Policy Option: 1a	Description: Provide for a maximum penalty of £50,000

COSTS

ANNUAL COSTS	
One-off (Transition)	**Yrs**
£ 135,000	10
Average Annual Cost (excluding one-off)	
£ 36,500	

Description and scale of **key monetised costs** by 'main affected groups'

ICO one off costs of around £100,000, covering items such as: staff training, printing material for publicity, promotion for stakeholders, updating websites.
Annual costs of around £25,000, including legal investigative costs, travel and subsistence, legal staff costs, legal costs (Counsel's fees, dealing with appeals from data controllers to the Information Tribunal, costs of recovering penalties through the courts). The ICO will not require further funding, because costs incurred by the introduction of this power will be covered by the additional money raised through tiered notification fees.
Tribunals: one off costs of around £35,000, which includes: amending the Tribunals Service website, guidance etc.
Annual costs of around £11,500, which includes the costs of hearings of appeals.

Total Cost (PV) **£ 450,000**

Other **key non-monetised costs** by 'main affected groups'

There will be no effect for those data controllers who continue to comply with their existing data protection obligations. Only data controllers who commit a serious contravention of the data protection principles may face a penalty. However the level of risk in which data controllers operate would be slightly increased. Overall compliance costs for data controllers would not change as a result of this option.

E F

ANNUAL BENEFITS	
One-off	**Yrs**
£	
Average Annual Benefit (excluding one-off)	
£ 300,000	

Description and scale of **key monetised benefits** by 'main affected groups'

Income would be raised by enforcing the penalties.

Total Benefit (PV) **£ 2.6 million**

Other **key non-monetised benefits** by 'main affected groups'

The main benefit of these proposals is greater compliance by data controllers, leading to greater public confidence in data handling practices. This increased confidence may encourage people to provide their details to bodies in both the public and private sectors.

Key Assumptions/Sensitivities/Risks

A key assumption is that the power to be brought into force will encourage a behavioural change in data controllers, especially those who knowingly or recklessly commit serious contraventions of the data protection principles. It is estimated that the ICO will impose 12 financial penalties per year of which three will be appealed in a First Tier Tribunal. It is also possible that the number of applications for good practice assessments could rise as data controllers may consider using it as a preventive measure. This would increase costs.

Price Base Year 2009	Time Period Years 10	**Net Benefit Range** (NPV) **-£135,000 to £10.7 million**	**NET BENEFIT** (NPV Best estimate) **£ 2.1 million**

What is the geographic coverage of the policy/option?				United Kingdom
On what date will the policy be implemented?				06.04.2010
Which organisation(s) will enforce the policy?				ICO/Tribunals/Courts
What is the total annual cost of enforcement for these organisations?				£36,500
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 NIL	Small NIL	Medium NIL	Large NIL
Are any of these organisations exempt?	No	No	No	No

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

Increase of £ NIL Decrease of £ NIL **Net Impact** £ NIL

Key:	**Annual costs and benefits: Constant Prices**	**(Net) Present Value**

Summary: Analysis & Evidence

Policy Option: 1b	Description: Provide for a maximum penalty of £500,000

COSTS

ANNUAL COSTS	
One-off (Transition)	**Yrs**
£ 135,000	1
Average Annual Cost (excluding one-off)	
£ 25,000	

Description and scale of **key monetised costs** by 'main affected groups'

ICO one off costs of around £100,000, covering items such as: staff training, printing material for publicity, promotion for stakeholders, updating websites.
Annual costs of around £17,500, including legal investigative costs, travel and subsistence, legal staff costs, legal costs (Counsel's fees, dealing with appeals from data controllers to the Information Tribunal, costs of recovering penalties through the courts). The ICO will not require further funding, because costs incurred by the introduction of this power will be covered by the additional money raised through tiered notification fees.
Tribunals: one off costs of around £35,000, which includes: amending the Tribunals Service website, guidance etc.
Annual costs of around £7,500, which includes the costs of hearings of appeals.

Total Cost (PV) **£ 345,000**

Other **key non-monetised costs** by 'main affected groups'

There will be no effect for those data controllers who continue to comply with their existing data protection obligations. Only data controllers who commit a serious contravention of the data protection principles may face a penalty. However the level of risk in which data controllers operate would be increased. Overall compliance costs for data controllers would increase following the introduction of a £500,000 maximum penalty.

E F

ANNUAL BENEFITS	
One-off	**Yrs**
£	
Average Annual Benefit (excluding one-off)	
£ 800,000	

Description and scale of **key monetised benefits** by 'main affected groups'

Income would be raised by enforcing the penalties.

Additionally, there would be direct benefits to society in terms of prevention of data mishandling as a result of increased deterrent effect of the ICO supervisory regime. Assuming for example four cases are prevented this could lead to benefits of around £48m.

Total Benefit (PV) **£ 6.9 million**

Other **key non-monetised benefits** by 'main affected groups'

The main benefit of these proposals is greater compliance by data controllers, leading to greater public confidence in data handling practices. This increased confidence may encourage people to provide their details to bodies in both the public and private sectors.

Key Assumptions/Sensitivities/Risks

A key assumption is that the power to be brought into force will encourage a behavioural change in all data controllers, especially those who knowingly or recklessly commit serious contraventions of the data protection principles. It is estimated that the ICO will impose eight financial penalties per year of which two will be appealed in a First Tier Tribunal. It is also possible that the number of applications for good practice assessments could rise as data controllers may consider using it as a preventive measure. This would increase costs.

Price Base Year 2009	Time Period Years 10	**Net Benefit Range** (NPV) **-£135,000 to £106.8 million**	**NET BENEFIT** (NPV Best estimate) **£ 6.5 million**

What is the geographic coverage of the policy/option?				United Kingdom
On what date will the policy be implemented?				06.04.2010
Which organisation(s) will enforce the policy?				ICO/Tribunals/Courts
What is the total annual cost of enforcement for these organisations?				£25,000
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 NIL	Small NIL	Medium NIL	Large NIL
Are any of these organisations exempt?	No	No	No	No

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

Increase of £ NIL Decrease of £ NIL **Net Impact** £ NIL

Key: **Annual costs and benefits: Constant Prices** **(Net) Present Value**

Summary: Analysis & Evidence

Policy Option: 1c	Description: Provide for a maximum penalty of £2.5 million

COSTS

ANNUAL COSTS	
One-off (Transition)	**Yrs**
£ 135,000	1
Average Annual Cost (excluding one-off)	
£ 20,000	

Description and scale of **key monetised costs** by 'main affected groups'

ICO one off costs of around £100,000, covering items such as: staff training, printing material for publicity, promotion for stakeholders, updating websites.
Annual costs of around £12,500, including legal investigative costs, travel and subsistence, legal staff costs, legal costs (Counsel's fees, dealing with appeals from data controllers to the Information Tribunal, costs of recovering penalties through the courts). The ICO will not require further funding, because costs incurred by the introduction of this power will be covered by the additional money raised through tiered notification fees.
Tribunals: one off costs of around £35,000, which includes: amending the Tribunals Service website, guidance etc.
Annual costs of around £7,500, which includes the costs of hearings of appeals.

Total Cost (PV)	£ 310,000

Other **key non-monetised costs** by 'main affected groups'

There will be no effect for those data controllers who continue to comply with their existing data protection obligations. Only data controllers who commit a serious contravention of the data protection principles may face a penalty. However the level of risk in which data controllers operate would be increased. Overall compliance costs for data controllers could increase significantly following the introduction of a £2.5 million maximum penalty.

E F

ANNUAL BENEFITS	
One-off	**Yrs**
£	
Average Annual Benefit (excluding one-off)	
£ 6 million	

Description and scale of **key monetised benefits** by 'main affected groups'

Income would be raised by enforcing the penalties.

Additionally, there would be direct benefits to society in terms of prevention of data mishandling as a result of increased deterrent effect of the ICO supervisory regime. Assuming for example six cases are prevented this could lead to benefits of around £72m.

Total Benefit (PV)	£ 51.6 million

Other **key non-monetised benefits** by 'main affected groups'

The main benefit of these proposals is greater compliance by data controllers, leading to greater public confidence in data handling practices. This increased confidence may encourage people to provide their details to bodies in both the public and private sectors.

Key Assumptions/Sensitivities/Risks

A key assumption is that the power to be brought into force will encourage a behavioural change in all data controllers, especially those who knowingly or recklessly commit serious contraventions of the data protection principles. It is estimated that the ICO will impose six financial penalties per year of which two would be appealed in a First Tier Tribunal. It is also possible that the amount of applications for good practice assessments could rise as data controllers may consider using it as a preventive measure. This would increase costs.

Price Base Year 2009	Time Period Years 10	**Net Benefit Range** (NPV) **-£135,000 to £537 million**	**NET BENEFIT** (NPV Best estimate) **£ 51.4 million**

What is the geographic coverage of the policy/option?				United Kingdom
On what date will the policy be implemented?				06.04.2010
Which organisation(s) will enforce the policy?				ICO/Tribunals/Courts
What is the total annual cost of enforcement for these organisations?				£20,000
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 NIL	Small NIL	Medium NIL	Large NIL
Are any of these organisations exempt?	No	No	No	No

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

Increase of £ NIL Decrease of £ NIL **Net Impact** £ NIL

Key:	**Annual costs and benefits: Constant Prices**	**(Net) Present Value**

Summary: Analysis & Evidence

Policy Option: 2a	Description: **Provide for a maximum penalty equal to 10% of the data controller's annual turnover or a maximum penalty of £500,000, if the percentage of turnover is not applicable to the data controller. Variant (a) Making information on annual turnover a registrable particular.**

COSTS

ANNUAL COSTS	Description and scale of **key monetised costs** by 'main affected groups'
One-off (Transition) **Yrs**	**ICO one off costs** of around £135,000, including items such as: staff training, printing material for publicity, promotion for stakeholders, updating website.
£ 170,000	**Annual costs** of around £17,500, they include legal investigative costs, travel and subsistence, legal staff costs, legal costs (Counsel's fees, dealing with appeals from data controllers to the Information Tribunal, costs of recovering penalties through the courts). The ICO will not require further funding, because costs incurred by the introduction of this power will be covered by the additional money raised through tiered notification fees.
	Tribunals: one off costs of around £35,000, which considers: amending the Tribunals Service website, guidance etc.
	Annual costs of around £7,500, which considers the costs of hearings of appeals.
	Data Controllers: Annual costs of around £2 million, which include approximate administrative costs of providing financial information to the ICO.
Average Annual Cost (excluding one-off)	
£ 2.0 million	**Total Cost** (PV) **£ 17.6 million**

Other **key non-monetised costs** by 'main affected groups'

Overall compliance costs for data controllers would increase following the introduction of a maximum penalty equivalent to 10% of annual turnover or up to £500,000.

E F

ANNUAL BENEFITS	Description and scale of **key monetised benefits** by 'main affected groups'
One-off **Yrs**	Income would be raised by enforcing the penalties.
£	Additionally, there would be direct benefits to society in terms of prevention of data mishandling as a result of increased deterrent effect of the ICO supervisory regime. Assuming for example four cases are prevented this could lead to benefits of around £48m.
Average Annual Benefit (excluding one-off)	
£ 800,000	**Total Benefit** (PV) **£ 6.9 million**

Other **key non-monetised benefits** by 'main affected groups'

In addition to increasing compliance by data controllers, leading to fewer data security breaches and reducing the costs associated with data security breaches, it would also lead to greater public confidence in data handling practices.

Key Assumptions/Sensitivities/Risks A key assumption is that the power to be brought into force will encourage a behavioural change in data controllers, especially those who knowingly or recklessly commit serious contraventions of the data protection principles. It is estimated that the ICO will impose eight financial penalties per year of which two will be appealed in a First Tier Tribunal. It is also possible that the amount of applications for good practice assessments could rise as data controllers may consider using it as a preventive measure. This would increase costs.

Price Base Year 2009	Time Period Years 10	**Net Benefit Range** (NPV) **-£17.6 million to £89.5 million**	**NET BENEFIT** (NPV Best estimate) **-£10.7 million**

What is the geographic coverage of the policy/option?			United Kingdom	
On what date will the policy be implemented?			06.04.2009	
Which organisation(s) will enforce the policy?			ICO/Tribunals	
What is the total annual cost of enforcement for these organisations?			£25,000	
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

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

Increase of £ **2 million** Decrease of £ **Net Impact** **£ 2 million**

Key: **Annual costs and benefits: Constant Prices** **(Net) Present Value**

Summary: Analysis & Evidence

Policy Option: 2b	Description: **Provide for a maximum penalty equal to 10% of the data controller's annual turnover or a maximum penalty of £500,000 , if the percentage of turnover is not applicable to the data controller. Variant (b) Giving the ICO the power to use the £500,000 maximum penalty when establishing the data controllers annual turnover is not possible.**

COSTS

ANNUAL COSTS	Description and scale of **key monetised costs** by 'main affected groups'
One-off (Transition) **Yrs**	**ICO one off costs** of around £100,000, covering items such as: staff training, printing material for publicity, promotion for stakeholders, updating websites.
£ 135,000	**Annual costs** of around £20,000, including legal investigative costs, travel and subsistence, legal staff costs, legal costs (Counsel's fees, dealing with appeals from data controllers to the Information Tribunal, costs of recovering penalties through the courts). The ICO will not require further funding, because costs incurred by the introduction of this power will be covered by the additional money raised through tiered notification fees.
	Tribunals: one off costs of around £35,000, which includes: amending the Tribunals Service website, guidance etc.
	Annual costs of around £7,500, which includes the costs of hearings of appeals.
Average Annual Cost (excluding one-off)	
£ 27,500	**Total Cost** (PV) **£ 365,000**

Other **key non-monetised costs** by 'main affected groups'

There will be no effect for those data controllers who continue to comply with their existing data protection obligations. Only data controllers who commit a serious contravention of the data protection principles would face a penalty. However the level of risk in which data controllers operate would be increased. Overall compliance costs for data controllers would increase following the introduction of a maximum penalty equivalent to 10% of annual turnover or up to £500,000.

BENEFITS

ANNUAL BENEFITS	Description and scale of **key monetised benefits** by 'main affected groups'
One-off **Yrs**	Income would be raised by enforcing the penalties.
£	Additionally, there would be direct benefits to society in terms of prevention of data mishandling as a result of increased deterrent effect of the ICO supervisory regime. Assuming for example 4 cases are prevented this could lead to benefits of around £48m.
Average Annual Benefit (excluding one-off)	
£ 800,000	**Total Benefit** (PV) **£ 6.9 million**

Other **key non-monetised benefits** by 'main affected groups'

In addition to increasing compliance by data controllers, leading to fewer data security breaches and reducing the costs associated with data security breaches, it would also lead to greater public confidence in data handling practices.

Key Assumptions/Sensitivities/Risks A key assumption is that the power to be brought into force will encourage a behavioural change in all data controllers, especially those who knowingly or recklessly commit serious contraventions of the data protection principles. It is estimated that the ICO will impose eight financial penalties per year of which two will be appealed in a First Tier Tribunal. It is also possible that the amount of applications for good practice assessments rise as more data controllers may consider using it as a preventive measure. This would increase costs.

Price Base Year 2009	Time Period Years 10	**Net Benefit Range** (NPV) **-£135,000 to £106.7 million**	**NET BENEFIT** (NPV Best estimate) **£ 6.5 million**

What is the geographic coverage of the policy/option?			United Kingdom	
On what date will the policy be implemented?			06.04.2009	
Which organisation(s) will enforce the policy?			ICO/Tribunals	
What is the total annual cost of enforcement for these organisations?			£27,500	
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

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

Increase of £ Decrease of £ **Net Impact** £

Key: **Annual costs and benefits: Constant Prices** **(Net) Present Value**

Summary: Analysis & Evidence

Policy Option: 2c	Description: **Provide for a maximum penalty equal to 10% of the data controller's annual turnover or a maximum penalty of £500 000, if the percentage of turnover is not applicable to the data controller. Variant (c) Creating a criminal offence through primary legislation for deliberately or recklessly providing the ICO with inaccurate turnover figures or not providing information at all**

COSTS

ANNUAL COSTS

One-off (Transition) **Yrs**

£ 135,000

Average Annual Cost (excluding one-off)

£ 31,000

Description and scale of **key monetised costs** by 'main affected groups'

ICO one off costs of around £100,000, covering items such as: staff training, printing material for publicity, promotion for stakeholders, updating websites.

Annual costs of around £23,500, including legal investigative costs, travel and subsistence, legal staff costs, legal costs (Counsel's fees, dealing with appeals from data controllers to the Information Tribunal, costs of recovering penalties through the courts). The ICO will not require further funding, because costs incurred by the introduction of this power will be covered by the additional money raised through tiered notification fees.

Tribunals: one off costs of around £35,000, which includes: amending the Tribunals Service website, guidance etc.

Annual costs of around £7,500, which includes the costs of hearings of appeals.

Total Cost (PV) **£ 400,000**

Other **key non-monetised costs** by 'main affected groups'

There will be no effect for those data controllers who continue to comply with their existing data protection obligations. Only data controllers who commit a serious contravention of the data protection principles may face a penalty and only those who refuse to provide information or provide inaccurate information to the ICO would be prosecuted. However the level of risk in which data controllers operate would be increased. Additionally there would be costs for the Courts as the ICO would prosecute data controllers for not providing information. Overall compliance costs for data controllers would increase following the introduction of a maximum penalty equivalent to 10% of annual turnover or up to £500,000.

E F

ANNUAL BENEFITS

One-off **Yrs**

£

Average Annual Benefit (excluding one-off)

£ 800,000

Description and scale of **key monetised benefits** by 'main affected groups'

Income would be raised by enforcing the penalties.

Additionally, there would be direct benefits to society in terms of prevention of data mishandling as a result of increased deterrent effect of the ICO supervisory regime. Assuming for example four cases are prevented this could lead to benefits of around £48m.

Total Benefit (PV) **£ 6.9 million**

Other **key non-monetised benefits** by 'main affected groups'

In addition to increasing compliance by data controllers, leading to fewer data security breaches and reducing the costs associated with data security breaches, it would also lead to greater public confidence in data handling practices.

Key Assumptions/Sensitivities/Risks A key assumption is that the power to be brought into force will encourage a behavioural change in all data controllers, especially those who knowingly or recklessly commit serious contraventions of the data protection principles. It is estimated that the ICO will impose eight financial penalties per year of which two will be appealed in a First Tier Tribunal. It is also possible that the amount of applications for good practice assessments rise as more data controllers may consider using it as a preventive measure. This would increase costs.

Price Base Year 2009	Time Period Years 10	**Net Benefit Range** (NPV) **-£135,000 to £106.6 million**	**NET BENEFIT** (NPV Best estimate) **£ 6.5 million**

What is the geographic coverage of the policy/option?			United Kingdom	
On what date will the policy be implemented?			06.04.2009	
Which organisation(s) will enforce the policy?			ICO/Tribunals	
What is the total annual cost of enforcement for these organisations?			£31,000	
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

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

Increase of £ Decrease of £ **Net Impact** £

Key:	**Annual costs and benefits: Constant Prices**	**(Net) Present Value**

Evidence Base (for summary sheets)

Introduction and Background

Organisations wishing to process personal data have since 1 March 2000 been under an obligation to comply with the DPA's data protection principles, which are:

- personal data shall be processed fairly and lawfully (and not to be processed unless specified condition(s) are met - additional conditions apply for sensitive personal data);
- personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes;
- personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed;
- personal data shall be accurate and, where necessary, kept up to date;
- personal data processed for any purpose or purposes shall not be kept longer than is necessary for that purpose or those purposes;
- personal data shall be processed in accordance with rights of data subjects under the DPA;
- appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data;
- personal data shall not be transferred to non-EEA countries without adequate protection.

The Information Commissioner's data protection responsibilities are funded by the notification fees paid to him by data controllers[1].

Following the significant losses of confidential personal data in 2007 calls were made by the general public and within Parliament to introduce a criminal offence for reckless or deliberate security breaches of personal data. The Government considered that a criminal offence would be a disproportionately heavy-handed penalty and an inadequate deterrent to regulatory non-compliance. Additionally, criminal proceedings could result in a costly and time-consuming process for data controllers and the ICO. The ICO agreed with Ministry of Justice (MoJ), that a civil penalty would be an appropriate alternative.

The ICO's power to impose Civil Monetary Penalties was inserted into the Data Protection Act 1998 (DPA) through section 144 of the Criminal Justice and Immigration Act 2008. Sections 55A to 55E contain the provisions regarding civil monetary penalties.

Between October 2007 to October 2008, 277 data security breaches were notified to the ICO, mainly IT-related loss/theft. These statistics provide examples which demonstrate the weakness of some organisations in processing data adequately and in full compliance with the data protection principles.

Mark Walport and Richard Thomas were asked to undertake a review of the framework for the use of personal information in the public and private sectors. After extensive consultation, they published the "Data Sharing Review Report" report in July 2008 which called for "significant improvement in the personal and organisation culture of those who collect, manage and share personal data", facilitated by a strong regulator with robust powers and sanctions.

[1] Notification is the process by which a data controller gives the ICO details about their processing of personal information. It is a statutory requirement and every organisation that processes personal information must notify the Information Commissioner's Office (ICO), unless they are exempt. Failure to notify is a criminal offence. Currently the notification fees are £35 for tier one and £500 for tier two data controllers.

The majority view among respondents to the Data Sharing Review, and in particular members of the public, was that "*the Data Protection Act should include stronger penalties and sanctions, and that the Information Commissioner should be given increased powers and resources to carry out his duties more effectively"*. There was wide support for the ICO's powers to be more akin to those of the Financial Services Authority (FSA), or the Health and Safety Executive; others argued for custodial sentences for some breaches. The FSA itself complained of the inequity of financial firms being penalised for their errors, when other organisations "*which may handle huge quantities of personal information, fall outside the regulatory regime*".

Data Sharing Review Recommendation 9 asked for the regulations under section 55A of the DPA to mirror the existing sanctions available to the FSA ("*high, but proportionate, maxima related to turnover*").

Consultation

A stakeholder event took place at the Ministry of Justice in October 2009 with representatives from the private and public sector. The majority of attendees supported the proposal of using a fixed maximum penalty of £500,000 and highlighted the need for clear guidance on how the Information Commissioner would use this power.

Additionally, between 9 November and 21 December 2009 the Ministry of Justice ran a public consultation on the maximum limit of Civil Monetary Penalties (CMPs). The document "Civil Monetary Penalties- Setting the maximum penalty" sought responses from data controllers (although the consultation was also open to the general public) to the question of whether a £500,000 maximum penalty was reasonable. The small majority of respondents were in favour of setting the maximum penalty at £500,000. The ICO considered that a £500,000 maximum penalty would provide a proportionate sanction whilst noting that a higher maximum penalty would provide a greater deterrent to large organisations and that the case for a higher maximum penalty should be kept under review. Details of the result of this consultation are contained in the Government response published on the Ministry of Justice website.

Policy Proposal

The DPA provides the ICO with an effective framework under which to regulate the DPA. However, the Government has decided to provide the ICO with an additional tool, which can both act as a deterrent - against non-compliance and also encourage data controllers to work with the ICO on compliance. This will contribute to increased compliance with the data protection principles and strengthen public confidence that data protection safeguards are observed.

Therefore, the Government is introducing regulations that will enable the ICO to impose financial penalties for serious breaches of the data protection principles.

Rationale for Government Intervention

Most data controllers comply with the data protection principles; however since misuse of even small amounts of personal data can have serious consequences, it is important to minimise non-compliance with the data protection principles as much as possible. As such, it is necessary to give the ICO the power to impose civil monetary penalties to ensure that those data controllers, who commit a serious contravention of the data protection principles, as described in section 55A of the DPA, are duly sanctioned. The penalty has to be meaningful, appropriate and act as a deterrent to other data controllers; therefore, we believe a financial penalty, in the form of Civil Monetary Penalty, is the most appropriate penalty. Similar powers are already in force in a number of EU Member States, including Spain where penalties of up to €600,000 can be imposed.

Financial penalties for non-compliance should provide a powerful deterrent for data controllers who may otherwise ignore their responsibilities under the DPA, as they will introduce a significant financial cost for data controllers. This should therefore increase compliance with the DPA.

Data losses cause costs for individuals, but these costs are not always borne by data controllers. In economic terms data controllers impose an externality on data subjects when a data loss occurs. Externalities are one form of market failure. Intervention in this case therefore confers efficiency benefits.

The DPA transposes EU Directive 95/46/EC. The current proposal is in line with the EU requirement set out in Article 24 of the Directive. This states that the "Member States shall adopt suitable measures to ensure the full implementation of the provisions in this Directive", in particular in relation to cases of infringement of the provisions.

Although the Government is introducing a new penalty, the activities that it could apply to are already considered contraventions of the law under the existing obligations to abide by the DPA. It therefore does not create a significant burden for data controllers, as their obligation to comply with the data protection principles and the DPA, is both pre-existing and continuing. The only change these regulations make is to create a new penalty for behaviour that is already prohibited.

Main affected groups

Any organisation that processes data will potentially be affected by these regulations. In 2009 there were about 319,000 data controllers registered on the public register of data controllers. These range from Central Government Departments and other public bodies to business of all sizes in the private sector. The chart below provides a breakdown of data controllers (approximate numbers) based on the ICO's public register:

Table 1

Type of Organisation	Approximate number of data controllers on Register
Public Sector	75,000
Private Sector	170,000
Third Sector	13,000
Unknown	44,000

What are the policy objectives and the intended effects?

Data breaches can have devastating effects on the public; they can lead to crime, distress, inconvenience and a lack of confidence in data controllers' ability to keep their data safe. Penalties for non compliance are likely to provide a powerful deterrent for data controllers who may otherwise ignore their responsibilities under the DPA. Sanctions currently available to the ICO under the DPA are mostly concerned with either ensuring future data controller's compliance with the DPA, or with bringing criminal charges.

We are introducing two statutory instruments which develop the framework established in sections 55A to 55E of the DPA. Following the provisions contained in the DPA, they have to be approved by Parliament through different procedures.

The deterrence provided by a potential penalty of £500,000 combined with the reputational risk attached to receiving a penalty should contribute to minimise the risk of any future serious

contraventions to the data protection principles. Ultimately this will help to restore public confidence in the security of personal data.

Although there will be no significant implementation costs for bringing this power into force, there will be operational costs which are discussed in detail below. The ICO estimates that there will be approximately 25 cases per year in which monetary penalties are imposed for serious contraventions of the data protection principles.

What policy options have been considered?

Two options have been considered:

Option 1 – Provide for a maximum penalty.
Three penalties were considered:
1a) £50,000
1b) £500,000
1c) £2.5 million

Option 2 – Provide for a maximum penalty equal to 10% of the data controller's annual turnover or a maximum penalty of £500,000; if the percentage of turnover is not applicable to the data controller.

We did consider the option of giving the ICO power to impose an unlimited penalty. This would have allowed the ICO to consider an appropriate level, relevant to the size of the company. However, as section 55A (5) of the DPA provides that *"the amount determined by the Commissioner must not exceed the prescribed amount",* this option has been discarded because the legislation requires a maximum amount to be set.

Cost Benefit Analysis

Base Case

Retain the status quo.
Maintaining the status quo means that there will be no changes to the current framework, and therefore no additional costs or benefits.

Option 1

Description
Data controllers that are deemed to have committed a serious contravention of the data protection principles could face a penalty of up to maximum amount set in regulations.

We considered three different maximum amounts: £50,000, £500,000 (our preferred option) and £2.5 million.

Option 1a)
Rationale for the £50,000 maximum figure
A maximum penalty of £50,000 provides a limited degree of deterrence against serious contraventions of the data protection principles. For some small data controllers, a maximum penalty of this magnitude would represent a significant risk. However, the same cannot be said of the rest of data controllers for whom this figure would not be meaningful in comparison with the resources they have, and may even be too low to be proportionate to the contravention. For many data controllers the risk of receiving a penalty would be worth taking, as they know that the likelihood of being issued with the highest maximum amount would be very low, and even in that case the costs could be absorbed by the business as a business cost. Considering this, we

think that this maximum amount would not represent a viable option, as its deterrent effect would be very limited.

Option 1b)
Rationale for the £500,000 maximum figure
In order for the penalty to be a fair but effective tool for the ICO, the level of penalty must be high enough to be an effective deterrent against potential contraventions of the data protection principles, but not disproportionate in relation to the financial resources of the majority of data controllers that might potentially be affected. We believe a penalty up to a maximum of £500,000 should act as a strong deterrent and additionally, consider it to be fair and proportionate for the large majority of data controllers.

We know that there are around 319,000 data controllers in the UK. However, there is only limited data on the sizes of organisations or their financial resources.

Available data about the type of data controllers and their size comes from research conducted for the purposes of changing the ICO's fee structure[2]. This research provided a good indication of the upper level of these data controllers only. It indicates that only around 5% of data controllers are either:

- private sector bodies with an annual turnover of more than £25.9 million and over 250 members of staff
- Public sector bodies with over 250 members of staff

The other 95% of data controllers are small, medium size data controllers, charities and other public bodies. However, it is not possible to establish the exact number of small or medium size private sector data controllers or the number of charities and public sector data controllers. Table 1 (in the Main Affected Groups section) provides the closest description of the number of data controllers by type.

There is a precedent set by other regulators such as OFCOM, OFFWAT and OFT, for using 10% of a sector specific definition of turnover as either the only indicator of the maximum level of penalty or in combination with a fixed maximum amount. We believe that although we are not using a percentage of annual turnover as our maximum penalty, the rationale behind its use – limit penalties to a reasonable and proportionate percentage of the company's resources - is still relevant for the purposes of setting a maximum penalty amount. In order to use this criterion we have estimated that the majority of the remaining 95% of private sector data controllers are likely to be companies that qualify as small companies -following the criteria used by the Department for Business Innovation and Skills. However, for the purposes of establishing a referential annual turnover, which is not too low to be ineffective for large data controllers, or too high in relation to small data controllers, we are using the turnover threshold between small and medium companies, which is £6.5 million.

Taking £6.5 million as the approximate turnover of the majority of private sector data controllers registered with the ICO, and considering the 10% of annual turnover as a guideline, and taking into account that the maximum penalty has to cover third and public sector data controllers as well, we concluded that a maximum penalty of £500,000 would be appropriate.

It is recognised that £500,000 may be seen as a relatively small financial penalty for larger data controllers. However, a comparison between this amount and maximum penalties at the disposal of other regulators in the UK and European Data Protection Regulators [3] shows that

[2] The ICO provided this information as part of his business case for changing the fee structure for notification. The new fee structure came into force on the 1 October 2009.
[3] See http://www.ico.gov.uk/global/search.aspx?collection=ico&keywords=Data+Protection+Powers+and+Penalties

this penalty would be one the highest (Spanish data protection authority can impose penalties of up to €600,000). Additionally, it is important to consider that a Civil Monetary Penalty is also likely to have a significant affect on the data controller's reputation. Reputational damage is likely to result in greater financial impact for larger data controllers in comparison to small and medium size data controllers. Therefore, a maximum £500,000 penalty is considered to be an effective deterrent against breaches of the data protection principles for all data controllers.

Safeguards
A £500,000 penalty could potentially impose undue financial hardship for some small data controllers. However, it should be noted that Section 55C of the DPA places an obligation on the ICO to produce guidance on the administration of monetary penalties. The ICO guidance on CMPs will contain provisions about the need for the penalty not to cause undue financial hardship on data controllers and the ICO's consideration of the likely impact of the penalty on the data controller, in particular financial and reputational impact.

The existence of an appeals procedure, which provides specific grounds for appealing the amount of the penalty, should also ensure that the penalties received for serious contraventions of the data protection principles are proportionate and reasonable.

The two to three year review period will enable the £500,000 figure to be revisited, if necessary. Any changes to the amount of the maximum penalty would be introduced through secondary legislation.

Option 1c)
Rationale for the £2.5 million maximum figure
We considered a maximum penalty of £2.5 million and concluded that it would also be an effective tool for the ICO, as it would provide with a significant and proportionate penalty for large data controllers.

In contrast with the £500,000 option, this figure appears to be disproportionately high in relation to the large majority of smaller data controllers potentially affected. While guidance should ensure that penalties are proportionate to the size of the data controller, it is possible in theory that the higher headline figure may lead some data controllers, especially those who are excessively risk averse, to significantly increase their overall compliance costs.

This potential risk of some smaller data controllers over-reacting to a higher maximum headline penalty could point towards adopting a lower maximum headline penalty, especially if larger data controllers place a large value on avoiding the negative publicity associated with having any penalty, even a small one

Costs of Option 1

Costs to Data Controllers

The threat of a penalty may encourage some data controllers who have not already done so, to ensure their systems are data protection compliant and may need additional resources to achieve this. These costs have not been quantified, but are likely to be greater the higher the maximum penalty is set. Government considers this proportionate as data controllers are already under a legal obligation to comply with the DPA. This is particularly the case as the DPA has been in force since 2000.

Data controllers can avoid a penalty by complying with the data protection principles. The ICO will be obliged under the terms of this guidance (which must be approved by the Secretary of State) to ensure that the level of any penalty must be proportionate, and not cause undue financial hardship.

Figures provided by the ICO state that from November 2007 to date there are almost 700 self reported breaches listed. Of these, 54 have resulted in the signing of a formal undertaking between the ICO and the CEO of the organisation concerned. Of these a significant number of the security breaches were serious breaches of the DPA and would have triggered the monetary penalty procedures.

Based on these figures, practical knowledge of the area, and the fact the CMPs are designed to be appropriate in only the most serious of cases; the ICO predict that they would use the power to issue a penalty no more than 25 times a year.

Since the level of penalty is assessed on a case by case basis, it is not possible to quantify what the average level of the penalty will be at this point If the maximum penalty was applied to the likely maximum number of times the penalty will be imposed (25 times), the maximum total cost to data controllers per year would be either £1.25 million (Option 1a)); £12.5 million (Option 1b)); or £62.5 million (Option 1c)). This cost would only be borne by those data controllers who breached the data protection principles. However, this scenario where the maximum penalty was imposed each time is extremely unlikely.

For the purposes of this Impact Assessment, a central scenario has been used. In this scenario, a penalty would be imposed 12 times per year, with a different average penalty depending on the policy option.

In summary therefore:

Option 1a)
Minimum cost (penalty) to data controllers: £0 (based on the existing obligation of 100% compliance with the data protection principles)

Central cost (penalty) to data controllers: £240,000 (based on 12 data controllers receiving a penalty of £25,000 as a result of their failure to meet existing data protection obligations).

Maximum cost (penalty) to data controllers: £1,250,000 (based on 25 data controllers receiving the maximum penalty as a result of their failure to meet existing data protection obligations).

Option 1b)
Minimum cost (penalty) to data controllers: £0 (based on the existing obligation of 100% compliance with the data protection principles)

Central cost (penalty) to data controllers: £800,000 (based on 8 data controllers receiving a penalty of £100,000 as a result of their failure to meet existing data protection obligations).

Maximum cost (penalty) to data controllers: £12.5 million (based on 25 data controllers receiving the maximum penalty as a result of their failure to meet existing data protection obligations).

Option 1c)
Minimum cost (penalty) to data controllers: £0 (based on the existing obligation of 100% compliance with the data protection principles)

Central cost (penalty) to data controllers: £6 million (based on 6 data controllers receiving a penalty of £1 million as a result of their failure to meet existing data protection obligations).

Maximum cost (penalty) to data controllers: £62.5 million (based on 25 data controllers receiving the maximum penalty as a result of their failure to meet existing data protection obligations).

It should be noted that costs to individuals or businesses that break the law are not scored in Impact Assessments as costs. Therefore, while these costs have been provided as indicative, they have not been scored as costs in the summary sheets.

Additionally, a data controller who wishes to make representations to the ICO against the imposition of a monetary penalty or to appeal a penalty would be faced with an additional burden in preparing such representations or the appeal. Government considers this proportionate, as only data controllers that the ICO believed were seriously contravening the data protection principles would be subject to a penalty.

Costs to the ICO
Since Civil Monetary Penalties are essentially a tool for the ICO to use in order to increase compliance with the data protection principles, the ICO is likely to incur costs with regards to implementation.

The ICO have provided estimates of the costs they are likely to incur. The one off costs are associated with administrative costs of enabling the use of the new policy. The annual costs however, will depend on the number of times that the ICO uses the penalty, and if the relevant data controller in each case chooses to use the appeals procedure.

As already stated, the ICO predict that they will use the penalty no more than 25 times per year. Of these 25, they expect

Option 1a)
No more than four cases to go to appeal in the First Tier Tribunal and of those a maximum of one case might go to the Upper Tier Tribunal.

Option 1b)
No more than five cases to go to appeal in the First Tier Tribunal and of those a maximum of one case might go to the Upper Tier Tribunal.

Option 1c)
No more than ten cases to go to appeal in the First Tier Tribunal and of those a maximum of three cases might go to the Upper Tier Tribunal.

The central scenario used in this Impact Assessment is based on 12 civil monetary penalties issued a year. So in the case of appeals going to the tribunals, the central case scenario would be of three appeals to the First Tier Tribunal (1a), two appeals to the First Tier Tribunal (1b), and two appeals to the First Tier Tribunal (1c).

We consider this to be a realistic assessment since in the last ten years, only six appeals by data controllers against the ICO have been heard by the Information Tribunal. This is likely to increase with the introduction of CMPs, as a potential financial penalty will increase the incentive for an appeal, and the bigger the penalty the more likely that the number of appeals would rise. The figures presented in this Impact Assessment are based on those projections.

Based on the ICO projections, ICO costs are estimated as follows:

Option 1a)
One off costs: £100,000
Annual costs: £25,000 in the central scenario. £52,000 in the high scenario.

Option 1b)
One off costs: £100,000
Annual costs: £17,500 in the central scenario. £52,000 in the high scenario.

Option 1c)
One off costs: £100,000
Annual costs: £12,500 in the central scenario. £52,000 in the high scenario.

It is important to note, that the ICO will be able to meet the cost within its existing budget. Additionally, the expected greater compliance with the data protection principles should reduce the number of cases that the ICO has to currently investigate. This in turn would reduce the ICO's investigative and legal costs associated with using the current framework which focuses on changing the behaviour of data controllers who are already contravening the data protection principles. As this policy is designed to change the behaviour of data controllers, greater compliance should reduce the need for this retrospective action.

Costs to Tribunals
It is difficult to predict the additional cost of these new appeals to the Tribunals Service since the current cases that are transferred to the High Court from the information tribunal will come under the jurisdiction of the new Upper Tier Tribunal as of January 2010.

Like the ICO however, the Tribunals Service predict that there will be initial administrative costs associated with implementation of the new policy and annual costs depend upon the number of cases they receive. Based on previous cases considered by the Information Tribunal, the average cost is around £3,800 per case. The average costs for the Upper Tier Tribunal are estimated to be around £1,500.

Based on the projections provided by the ICO, and information provided by the Tribunal Service, the costs to the Tribunals are estimated as follows:

One off costs: £35,500
Implementation costs (e.g. IT, judicial training, staff training)

Option 1a)
First tier Tribunals
Annual costs: £11,500 in the central scenario. £15,000 in the high scenario.

Upper Tier Tribunals
Annual costs: £1,500 in the high scenario.

Option 1b)
First tier Tribunals
Annual costs: £7,500 in the central scenario. £23,000 in the high scenario.

Upper Tier Tribunals
Annual costs: £1,500 in the high scenario.

Option 1c)
First tier Tribunals
Annual costs: £7,500 in the central scenario. £38,000 in the high scenario.

Upper Tier Tribunals
Annual costs: £4,500 in the high scenario.

Benefits of Option 1
Since Civil Monetary Penalties are designed to work as a deterrent it is difficult to quantify the potential benefits. There are however, a number of areas where their existence is likely to have a positive effect.

Penalty revenue
Revenue will be raised from penalties imposed. As outlined above, the level of penalties will be set to be proportionate, meaning it is difficult to accurately predict the volume of penalty income likely to be received. Based on case volumes and depending on the maximum penalty, the range of possible income is between zero and £62,500,000 per year.

For modelling purposes, a central projection is that around 12 cases per year would occur. We have used an average value of the maximum penalty to calculate revenue for each option.

Option 1a)
£300,000 based on 12 data controllers receiving a penalty of £25,000.

Option 1b)
£800,000 based on eight data controllers receiving a penalty of £100,000.

Option 1c)
£6 million based on six data controllers receiving a penalty of £1 million.

Wider Society

The existence of CMPs is likely to encourage greater compliance with the data protection principles. Greater compliance with the principles should contribute to a higher level protection of personal data and a reduction in the costs associated with data breaches, such as identity theft. It is difficult to estimate precisely how many data breaches of the DPA may be prevented as a result of the deterrent effect of CMPs. In addition, there is no definitive assessment of how much mishandling of data costs organisations. However, research carried out by the Ponemon Institute in 2008 suggested that each data breach cost an organisation an average of £1.73 million. Each record lost costs a firm an average of £60, of which £32 was in lost business following the data loss[4]. 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[5].

Net Impact
The monetised costs and benefits of Option 1 are set out above, leading to an estimated net benefit of around

£2.1 million overall benefit for **Option 1a)**

£6.5 million overall benefit for **Option 1b)**, and

£51.4 million overall benefit for **Option 1c)**.

There are also non monetised benefits associated with this option and each of its variants. Option 1b) is the preferred option.

Option 2

Description
Where the data controller is a specified legal person such as a Public Limited Company, and has a turnover based on the definition found in the Companies Act 2006, the prescribed

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

5 ICO press release 18 June 2009 'Putting a price on privacy protection'

maximum amount could be no more than 10% of the data controller's most recent annual turnover; but if a data controller does not have a turnover, or if it is exempt from a turnover-based maximum, a penalty up to a maximum of £500,000 could be imposed.

Difficulties of working with turnover:

- Approximately 319,000 data controllers are listed on the ICO's public register. The ICO does not currently have access to the turnover information of data controllers and there seems to be no single source from which the ICO could easily obtain turnover information, or information that could be used to deduce turnover, for all data controllers.

- Data controllers may encompass more than one business or organisation in its registration before the ICO. For example, MoJ's registration as a data controller includes a number of subsidiary bodies. Large companies may also register as a single data controller for all branches of their business, but under company law this enterprise could comprise a number of subsidiaries and numerous branches with individual turnovers.

- Self-employed persons may have more than one business interest. Not all business interests might involve personal data but they will only have a single total income. Using this total income to calculate the maximum penalty in such circumstances would seem unfair. There is also no definition of turnover for sole traders.

- Companies that are newly created and so do not yet have a reported or calculated turnover, as well as companies that have a limited turnover due to the nature of their business, will not be appropriately covered by this option. For example, if a recently created internet company whose sole business involved storing personal data on its server committed a breach warranting a significant penalty, but only had a turnover of £1000, then the ICO would be limited to a maximum penalty of £100. This would seem to be disproportionately low.

- It may not be practical to base the maximum penalty on turnover for data controllers who form part of multinational organisations or branches of international organisations. International reporting and filing requirements for companies differ from country to country, and in any case, figures obtained from those sources are unlikely to reflect the turnover of the enterprise that is registered as a data controller in the UK. The international reporting requirements also vary depending on the size and legal form of the company (sole proprietorship, partnership, limited liability etc), and these in turn differ from our own UK definitions.

Due to the complexities briefly outlined above, and the potential difficulties for the ICO to obtain information about turnover, we considered three different ways of ensuring the workability of this option:

Option 2a)
Making information on annual turnover a registrable particular.
Turnover could be prescribed through secondary legislation as a registrable particular. This would require all data controllers who register with the ICO to calculate and report their turnover, where applicable, to the ICO each year, when their notification with the ICO was renewed. The ICO could then use this information to determine the maximum penalty for each relevant data controller.

Risks and difficulties

- Requiring all data controllers to calculate, according to a specific definition, and provide their latest annual turnover figure would constitute an administrative burden for data controllers of all sizes.

- This variant would also represent an administrative burden for the ICO, who would need to collect and retain the additional information in line with the data protection principles, ensuring the data remained accurate, up to date and not excessive.
- This variant might also be regarded as disproportionate given the number of times the penalties are likely to be used in contrast to the burden this option would impose on many data controllers each year.

Option 2b)
Giving the ICO the power to use the £500,000 maximum penalty when establishing the data controller's annual turnover is not possible.
Giving the ICO the power -through secondary legislation- to ask data controllers for their turnover when the ICO intends to impose a CMP. If the information was not forthcoming, the ICO could try to establish turnover by contacting Companies House. If the ICO was unsuccessful in establishing turnover, a maximum penalty of £500,000 could be imposed.

Risks and difficulties

- It would be ineffective without a sanction in the event that the data controller refused to provide the information to the ICO. It is possible that section five of the Perjury Act 1911 could be used if a data controller deliberately provided a false turnover. However, this does not solve the problem of data controllers providing the wrong information in good faith, or of data controllers who continually delay or refuse to provide the information.
- The request for turnover could be considered to be an unexpected use of the power set out in section 55E.
- If the ICO was unable to assess a data controller's turnover, the prescribed fixed maximum could be applied. However, if the maximum amount is set at £500,000, any data controller with an annual turnover greater than £5 million might be discouraged from providing the relevant details to the ICO because they might then be issued with a penalty of a higher amount.

Option 2c)
Creating a criminal offence -through primary legislation- for deliberately or recklessly providing the ICO with inaccurate turnover figures, or not providing information at all.
Giving the ICO the power to request turnover information from a data controller, coupled with an enforcement mechanism in primary legislation (creating a criminal offence); if the data controller refused to provide the information or provided inaccurate information. So, data controllers could have been prosecuted for either not providing information about turnover or for providing inaccurate information deliberately.

Risks and difficulties

- Likely to face strong opposition from the private sector in response to an additional criminal offence targeted at businesses.
- It does not solve the problem of obtaining information on turnover or providing the ICO with an adequate scheme to impose civil monetary penalties.

Costs of Option 2

Costs to data controllers
The threat of a penalty may encourage some data controllers who have not already done so, to ensure their systems are data protection compliant and may need additional resources to achieve this. All variants in Option 2 have an alternative maximum penalty of £500,000; hence the costs to business will be equivalent to those under Option 1b.

Data controllers' administrative burdens
Annual costs would also be generated in Option 2a for those data controllers who have a turnover based on the definition found in the Companies Act 2006, as they would need to submit this information as part of their annual notification to the ICO. We estimate that there are around 170,000 data controllers that would be obliged to notify and that the additional time required to comply with this new obligation would be of around 30 minutes.

Considering the amount of time per data controller, the approximate number of data controllers obliged to notify, and a wage rate of £23.40 per hour[6]; we estimate the annual cost across all data controllers would be around £2 million.

ICO
The ICO costs are estimated as follows:

Option 2a)
One-off costs of around £135,000. The ICO would need to make amendments to notification policies and procedures, update the ICO website, and issue new guidance on registrable particulars.

Annual costs of around £20,000 in the central scenario. £60,000 in the high scenario.
Central scenario costs increase as this option requires use of resources independently of the number of civil monetary penalties issued a year.

Option 2b)
One-off costs of around £100,000

Annual costs of around £20,000 in the central scenario. £60,000 in the high scenario.
It considers among other items, additional investigative resources the ICO would need to obtain information on turnover.

Option 2c)
One-off costs of around £100,000

Annual costs of around £23,500 in the central case. £70,000 in the high scenario.
The additional costs would be generated mainly as a consequence of the ICO having to expend more resources prosecuting those data controllers who didn't provide the information required.

Costs to Tribunals
Similar to those estimated for Option 1b). This is:

One off costs of £35,000

First tier Tribunals
Annual costs: £7,500 in the central scenario. £23,000 in the high scenario.

Second tier Tribunals
Annual costs: £1,500 in the high scenario.

Benefits of Option 2
The benefits of Option 2 would be the same as those set out in Option 1c), for the three options.

[6] Information obtained from the MoJ admin burden database.

Net Impact of Option 2
The monetised costs and benefits of Option 2 are set out above, leading to an estimated net benefit of around

£10.7 million overall **cost**, for **Option 2a)**

£6.5 million overall benefit, for **Option 2b)**, and

£6.5 million overall benefit for **Option 2c)**.

There are also non monetised benefits associated with this option and each of its variants.

Specific Impact Tests

Competition Assessment
No measurable competition impact is foreseen.

Small Firms Impact Test
Retaining the status quo has no impact on small firms as present.

Options (1) and (2) may impact some small businesses, if they receive a financial penalty, but this will only apply to businesses who are failing to comply with existing legal obligations. However, as the level of the penalty determined by the Information Commissioner would take into account, among other things, financial resources of the data controller, small firms should not be impacted disproportionately.

During the consultation on the maximum limit of CMPs concerns were raised about the potential impact on small firms when this penalty is introduced. Careful consideration has been given to this matter and it would appear that there will be no significant impact on small business from penalties because data controllers are not required to do anything new.

To help data controllers understand their responsibilities and what they need to do to comply with the DPA, the ICO provides extensive guidance on his website, The ICO's statutory guidance on CMPs sets out the ICO's interpretation of how the legal provisions on CMPs will be applied in practice.

In addition the ICO published in November 2009 "the Guide to data protection", which provides clear guidance on data controllers' responsibilities under the DPA. This coupled with other sources of advice available to small businesses on data protection issues (the ICO's help line, specific guidance on different data protection issues etc) will support small firms in understanding their data protection responsibilities and so help reduce the burden of compliance with the DPA.

Legal Aid/Judicial Impact
Retaining the status quo will have no additional impact on legal aid/judicial resources than at present.

No legal aid costs are estimated for this policy, because legal aid is not provided for data protection cases going to the First Tier Tribunal. In the case of the Upper Tier Tribunal, it is also very unlikely that legal aid would be provided for data protection cases. The likely legal aid costs from the Upper Tier Tribunal would be very low considering that only one case a year may be heard by this tribunal (as estimated by the ICO).

Options (1) and (2) will have a marginal impact on the Courts, as appeals against the new penalty will lie with the First Tier Tribunal and further appeals will lie with the Upper Tier Tribunal. The ICO estimates that almost no further appeals would go to the Courts, this is based in historical figures, which show that there have been only five appeals to the High Court in the past seven years, this is less than one appeal per year. Considering that the cases heard by the High Court will be heard by the Upper Tier Tribunal from January 2010, the likelihood of cases going to the Courts is considered to be minimal.

The ICO considers that a maximum of five cases per year may need to be taken to court for recovery of the penalty. However these cases will not generate any additional costs to the Courts, because recovery of penalties in the Courts must be done following a civil proceeding for which the ICO has to pay fees. These fees cover the costs the Court has to incur as a consequence of the proceedings.

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.

Others

There are no anticipated environmental, health or rural impacts resulting from this policy

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	*Results in Evidence Base?*	*Results annexed?*
Competition Assessment	Yes	No
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	Yes	Yes
Disability Equality	Yes	Yes
Gender Equality	Yes	Yes
Human Rights	Yes	Yes
Rural Proofing	Yes	No

Annex
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

Bringing into force the Information Commissioner's power to issue a civil monetary penalty of up to £500,000 against any data controller who: a) deliberately commits a serious contravention of section 4(4) of the Data Protection Act 1998 (DPA) which is likely to cause substantial damage or substantial distress b) commits a contravention of section 4(4) of the DPA which is likely to cause substantial damage or substantial distress and they knew or ought to have known that: b.1) there was a risk that the contravention would occur and b.2) such contravention would be of a kind likely to cause substantial damage or substantial distress but failed to take reasonable steps to prevent the contravention.

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

Victor Riega, 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	**Outcomes**
To enhance the regulatory powers of the Information Commissioner's Office (ICO) as provided for by the DPA. This power will enable the ICO to impose financial penalties for serious contraventions of the data protection principles. This will provide a deterrent against non-compliance by data controllers and an effective sanction in the event of serious contraventions.	The power to be brought into force should encourage a behavioural change in those data controllers who knowingly or recklessly commit serious contraventions of the data protection principles. One of the likely effects of bringing into force this power will be that data controllers would be encouraged to approach the ICO when they are concerned that their data processing may not be compliant with the DPA. The existence of this power should contribute to a higher level of protection of personal data, which in turn is likely to contribute towards addressing public concerns about how their data are protected.

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

Current Impact Assessment of bringing into force the ICO's power to impose civil monetary penalties Outcomes of the Ministry of Justice Stakeholder Event on Civil Monetary Penalties (12 October 2009) Data Sharing Review Report (July 2008) ICO Annual Report (July 2009) Outcome of public consultation "Civil Monetary Penalties-Setting the maximum penalty" (9 November-21 December)

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?

After considering information from various sources, such as those listed above at Q.4, we are satisfied that we have sufficient information.

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?

There are no positive impacts on the different groups of people. The ICO would be able to issue a civil monetary penalty on any data controller, and no distinction is made between groups. The emphasis is on data protection practices and not on the individual circumstances of data controllers. Data controllers may be affected by this power only if they commit a serious contravention of the data protection principles.

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

No. The ICO's power to impose civil monetary penalties would cover all data controllers and there are no disadvantageous effects on one particular group.

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

No adverse equality impact has been identified. Although the current proposal introduces a new penalty, the activities that it may be applied in response to are already considered contraventions of the law. The only change this proposal makes is to create a new penalty for behaviour that is already prohibited.

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

No.

10. Is a full Equality Impact Assessment Required? **No**

We have not identified any specific equality impacts in relation to these proposals and therefore will not carry out a full impact assessment.

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.

We plan to review the maximum penalty (£500,000) three years after implementation. However, if any unfair treatment of certain groups is identified before this, we will work to rectify this as soon as practicable.

12. Name of Senior Manager and date approved

This EIA relates to the implementation of the Information Commissioner's power to impose civil monetary penalties on data controllers who commit a serious contravention of the data protection principles, as described in section 55A of the DPA. Financial penalties for non-compliance should provide a powerful deterrent against such contraventions and should therefore increase compliance with the DPA. No positive or negative impacts have been identified.
Name: Belinda Lewis
Department: Ministry of Justice
Date: 04/01/09