



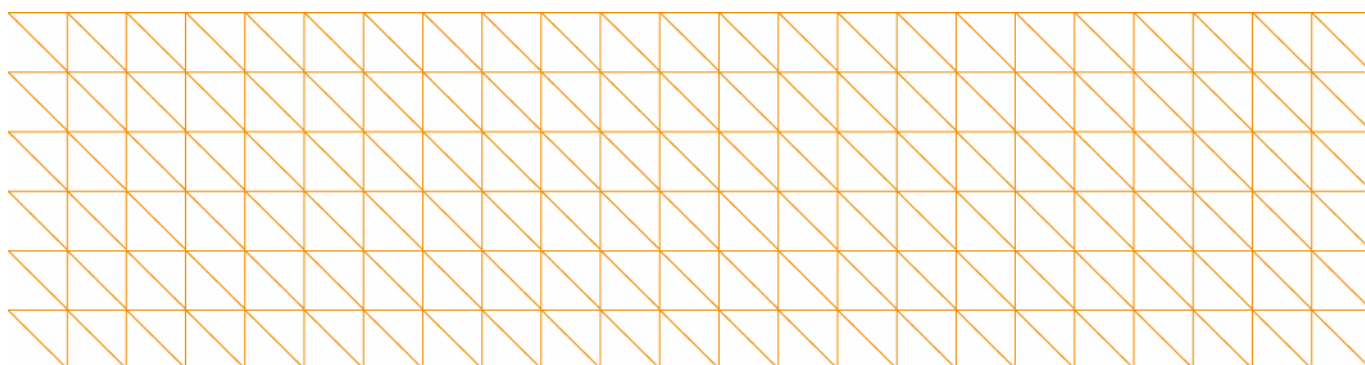
Ministry of  
**JUSTICE**

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

## **Summary of responses**

**Response to Consultation Paper CP(L) 15/08**

24 November 2008





Ministry of  
**JUSTICE**

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

**Response to consultation carried out by the Ministry of Justice.**

**This information is also available on the Ministry of Justice website:  
[www.justice.gov.uk](http://www.justice.gov.uk)**

## Contents

Introduction and contact details	3
Background	4
Summary of responses	7
Response to specific questions	
• Assessing good practice	8
• Inspection powers	13
• Funding	19
Conclusion	22
Glossary	23
Consultation co-ordinator contact details	25
The consultation criteria	25
Annex A – List of respondents	26

---

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

## Introduction and contact details

This document is the post-consultation report for the consultation paper, 'The Information Commissioner's inspection powers and funding arrangements under the Data Protection Act 1998'.

It will cover:

- background to the report;
- a summary of the responses to the report;
- a response to the specific questions raised in the report and
- conclusions, including the next steps.

Further copies of this report and the consultation paper can be obtained by contacting **Matthew Benson** at the address below:

**Matthew Benson**  
**Information Directorate, Ministry of Justice**  
**102 Petty France**  
**London**  
**SW1H 9AJ**

**Telephone: 020 3334 3769**  
**Email: [matthew.benson@justice.gsi.gov.uk](mailto:matthew.benson@justice.gsi.gov.uk)**

**This document is available on the Ministry's website: [www.justice.gov.uk](http://www.justice.gov.uk)**

## Background

The world in which regulators operate continues to change both with the pressure on business of a more competitive world, and the changing regulations that need to be enforced. As a society, we have increased expectations that regulations can and will protect consumers, businesses, workers and the environment, coupled with an increasing need to keep our businesses efficient and flexible to face new competitive challenges. As part of this, it is the role of the Information Commissioner's Office (ICO) to assess compliance with and enforce the Data Protection Act 1998 (DPA). The ICO has linked but separate roles in assessing compliance and enforcement. These regulatory roles sit at either end of the spectrum of options available to the ICO in discharging its responsibilities, and it is important that the two should not be confused. It should remain for the ICO to judge where on that spectrum their activity begins and ends with regard to individual data controllers based on their assessment of the issues at hand.

We believe that, although the current regulatory framework does not require sweeping changes, more can be done to ensure that the ICO has appropriate powers and tools to regulate an effective data protection and data-sharing regime in the UK. These tools must be flexible enough to meet a range of circumstances, to encourage good practice but allow firm and assertive action where necessary.

The consultation paper 'The Information Commissioner's inspection powers and funding arrangements under the Data Protection Act 1998' was published on 16 July 2008. It invited comments on a recommendation of the Data Sharing Review<sup>1</sup> published on 11 July, which was that the ICO requires stronger powers and sanctions to carry out its duties as an effective regulator and in order to facilitate this, greater funding.

The amendments outlined below, used rigorously and effectively in conjunction with the ICO's current powers, should enable it to regulate our data protection laws effectively at the same time as increasing public trust in how data is handled by organisations in the private and public sectors.

Our response to this consultation process has been aimed at ensuring, insofar as possible, that alterations to the regulatory framework reflect the Government's Better Regulation Executive code of practice and the five key principles of regulation identified in the Arculus review<sup>2</sup>. These principles are the cornerstone of the Government's better regulation strategy that state regulation should be:

---

<sup>1</sup> Report of the Data Sharing Review

<sup>2</sup> The Arculus Review "*Regulation - Less is More: Reducing Burdens, Improving Outcomes*"

- **Transparent** in enforcing the law and securing compliance
- **Accountable** for decisions and approaches taken
- **Proportionate** so data controllers know what to expect
- **Consistent** in approach and
- **Targeted** at cases where enforcement action is required.

We agree with the Hampton Review<sup>3</sup> that efficient enforcement supports compliance with legislation, assisting to deliver targeted and effective regulation without unreasonable administrative cost to business.

As part of a package of measures to increase compliance with the DPA and to contribute toward protecting people's personal data more effectively, the Ministry of Justice proposes:

- to legislate to exempt data controllers who consent to a Good Practice Assessments (GPA), should a breach be found as part of that GPA, from the new monetary penalty at section 55A DPA
- to legislate to include an explicit time limit for the provision of information to the ICO under a section 43 notice
- to legislate to enable the ICO to require any person on the premises, where a warrant is being executed, to provide the ICO with any information as appropriate to that investigation
- to revise the funding structure for the ICO's DPA work to a tiered notification fee from data controllers based on size of organisation
- that the ICO considers introducing self-assessment audit packs, should an organisations request them to assess their own compliance with the DPA
- that the ICO considers creating, monitoring and managing a 'Good Practice Forum' on its website, allowing the ICO and data controllers to disseminate good practice more widely and effectively
- that the ICO simplifies its registration form and process where possible and
- that the ICO consider allowing online payment of the notification fee.

---

<sup>3</sup> The Hampton Review *"Reducing administrative burdens: effective inspection and enforcement"*

In addition, the Ministry of Justice proposes to legislate to allow the ICO to undertake GPA of public sector data controllers without requiring consent from the organisation in question.

In support of the recommendations above, we anticipate that the ICO will publish clear and understandable guidance to ensure data controllers are informed of the practical implications, process and consequences of these changes.

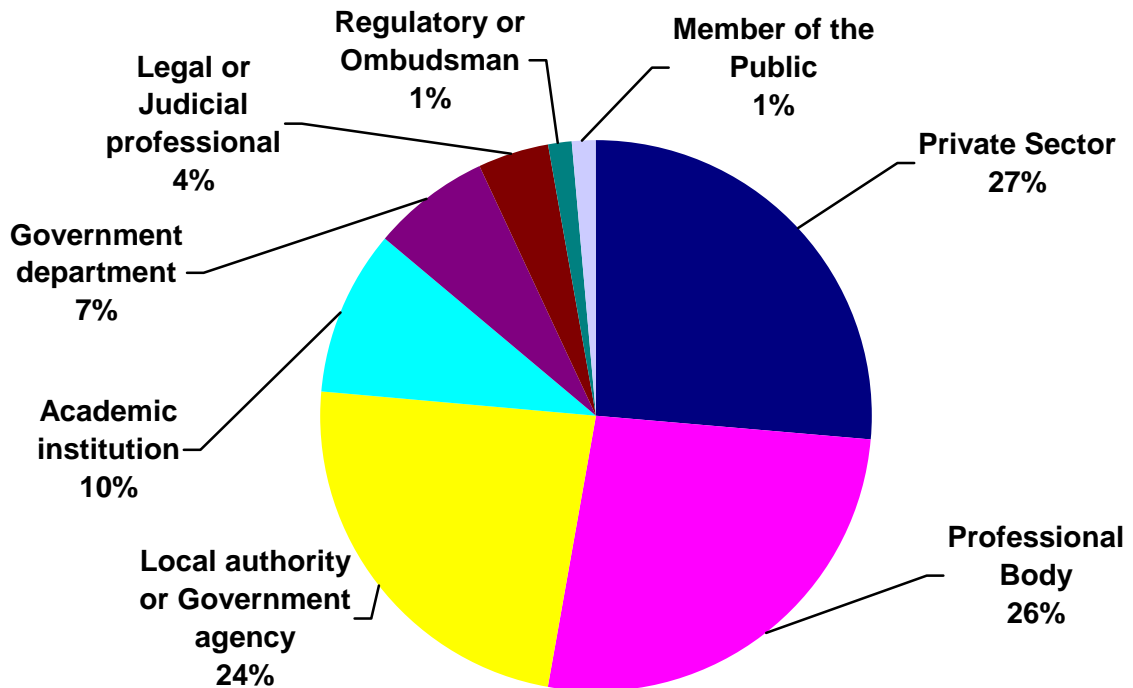
This report summarises the responses to the consultation, which closed on 27 August 2008, including how the consultation process influenced the final decisions reached.

We also held a stakeholder event on some of the recommendations from the Data Sharing Review and our proposals that supplemented the written consultation. A wide range of representatives attended including large and small private sector businesses, central and local government, trade associations and professional bodies. The feedback we received was on the whole very positive and has helped to inform this response.

A list of respondents to our consultation paper is at Annex A.

## Summary of responses

A total of 72 responses to the consultation were received; the breakdown of these responses by sector is indicated below.



The responses were analysed for possible new approaches to address the issues involved, evidence of the impact of the proposals, levels of support and any key observations from both those who agreed with and those who did not agree with the proposals.

With the exception of the proposal allowing the ICO to enter all premises without consent or evidence, our proposals were received positively by a majority of respondents. Those in favour of these proposals provided helpful comment and input as to the practicality of the proposals, including suggestions on how they could best be implemented.

## Assessing good practice

A GPA is part of a range of regulatory tools available to the ICO. It is a focused and specific assessment, not necessarily always occurring on site. The ICO's current powers in relation to assessing good practice by data controllers with the DPA are covered by section 51(7) that states:

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

A GPA is used as an incentive to enhance compliance by promoting a better understanding of the responsibilities of a data controller and improves practices and procedures. It should enable a data controller to demonstrate compliance, allowing an opportunity to rectify procedures that may not be fully compliant with the DPA. A GPA is not a punitive measure but a collaborative approach to assessing good practice that ultimately benefits data controllers and the data subjects whose information is processed.

It is therefore essential that a GPA is designed and conducted proportionately in a way that benefits data controllers and data subjects. Should the process of consenting to a GPA substantially increases the burden on data controllers, that burden will act as a deterrent, which would not serve the interests of data subjects. Added administrative and financial burden to business of a wide-ranging GPA would not be acceptable; the benefits of a GPA to a data controller, and therefore to data subjects and the public at large, should not be eroded by the burden of consenting.

Government is committed to ensuring personal data is protected in accordance with the DPA and consider GPAs an essential part of that process. On 21 November 2007, the Prime Minister gave 'the Information Commissioner the power to spot-check Government Departments, to do everything in his power and our power to secure the protection of data'.<sup>4</sup> As a result of this commitment and the recent Cabinet Office review of data handling in Government<sup>5</sup>, a system for the ICO to conduct GPAs across all central Government departments is being put in place. The first central Government GPA is currently under way.

---

<sup>4</sup> Prime Minister's Questions – Wednesday 21 November 2007

<sup>5</sup> Cabinet Office Report on *"Data Handling Procedures in Government: Final Report"*

**Proposal 1 - That data controllers should have the opportunity to provide consent for a Good Practice Assessment when registering with the ICO and**

**Proposal 2 - A three-month notice period for data controllers to withdraw consent for a Good Practice Assessment.**

### Responses

	<b>Proposal 1</b>	<b>Proposal 2</b>
<b>Yes</b>	53 (73%)	45 (62%)
<b>No</b>	9 (13%)	12 (17%)
<b>No answer</b>	10 (14%)	15 (21%)

There was overwhelming support for advance consent to GPAs, with respondents viewing them as a sensible and efficient measure. The proposal made sense to the Association of Chief Police Officers (Scotland), it would allow a simple mechanism for registering interest in undertaking a GPA. Halifax Bank of Scotland considered that the proposal would be an efficient means of obtaining consent. Both Liberty and Friends Provident thought this proposal would streamline the current process. The Department for Work and Pensions said this should encourage and have a positive effect on compliance with the DPA. The Birmingham and Solihull Mental Health Foundation Trust felt that this would improve the efficiency of the process.

The ICO understood the rationale for allowing advance consent for a GPA but were concerned about adding complexity to the system and running counter to the Hampton requirements for fewer forms.

A large proportion of respondents thought a notice period for withdrawal of consent to a GPA was appropriate and would act as an effective measure to avoid abuse of the system; ensuring consent can not be withdrawn once a GPA is arranged. Newcastle University, Datpro Ltd and the Environment Agency thought a three-month notice period was reasonable, valid and sensible respectively.

## Outcome

A GPA is rightly a collaborative process and we need to ensure the methodology of a GPA sends out the right signal to data controllers in relation to compliance. For the reasons outlined above, and given the Hampton recommendation that inspections should not occur without justification, we conclude that consent should be provided, as standard, before the ICO undertakes a GPA.

The majority of respondents agreed there is merit in seeking consent at the point of registration or re-registration with the ICO. We also note the comments relating to streamlining the current process and consider this the most effective way to gain consent. However, given the current concerns of the ICO and a possible potential increase in burden on business we do not propose the ICO take this forward at this stage.

Although the DPA does not generally distinguish between the public and private sector in this case such a distinction is vital. We are conscious of imposing further burdens on business, but more significantly we must consider the nature of the information held and processed by the public sector. It is essential to protect the rights of every data subject and to ensure their confidence in public authorities that their personal data is safeguarded. We can and must do all that we can to ensure personal data is handled securely.

We therefore propose to allow the ICO to carry out GPAs on public authorities without necessarily requiring prior consent. This builds on the Prime Minister's undertaking last year to open up Government departments to inspection by the ICO and recognises the different circumstances of private sector data controllers from those in the public sector. We propose to legislate to extend the Prime Minister's undertaking to public authorities in the UK. We plan to work with the devolved administrations to ensure that the proposals are applied to all relevant public authorities consistently across the UK.

If the ICO is not allowed to assess compliance, whether by a public or private sector data controller, this refusal or withdrawal of consent and any reason provided, should be taken into consideration in deciding whether to undertake enforcement action. By increasing the use of ICO powers to assess good practice and changes to the requirement for the consent of public authorities the ICO will continue to have a strong but proportionate set of regulatory powers to ensure compliance and good practice.

In light of our response to Proposal 1, we recommend the ICO consider how the withdrawal of consent, or the denial of access, under a GPA, will be factored into the consideration of enforcement action.

**Proposal 3 - To exempt data controllers who consent to a Good Practice Assessment from the civil monetary penalty under section 55A of the Data Protection Act 1998 (DPA) (once in force) for a breach discovered in the process of a Good Practice Assessment.**

**Responses**

	<b>Proposal 3</b>
<b>Yes</b>	52 (72%)
<b>No</b>	12 (17%)
<b>No answer</b>	8 (11%)

A large majority of respondents to the consultation agreed with this proposal. Those in favour considered it would provide an effective incentive, contributing to ensuring good practice would be observed by data controllers and allowing an increase in compliance without fear of recrimination.

Experian considered this proposal would ensure a GPA was a joint approach rather than a punitive measure. The Association of British Insurers stated that if a data controller were not immune from civil monetary penalties, then this would discourage initial consent.

**Outcome**

There are real benefits to organisations for participating in a GPA and Government wants to encourage all organisations to work with the ICO in this way by providing an incentive.

Government proposes to legislate to exempt a data controller who has consented to a GPA from the new civil penalty should a breach of the DPA be found in the course of that assessment. The ICO will, however, retain the power to use existing powers to issue Enforcement and Information Notices and powers to undertake prosecutions.

This measure is designed to promote good practice, allowing data controllers to invite scrutiny, safe in the knowledge that no penalty would be imposed for problems identified.

## **Additional recommendations**

**Introducing self-assessment audit packs:** King's College London suggested the ICO should produce self-assessment packs for completion. This proposal has a great deal of merit, in particular the possibility for increasing awareness of compliance by data controllers. Such a pack would complement the ICO's existing guidance on conducting an audit of compliance. We recommend that the ICO produce self-assessment audit packs, should an organisation request them to assess compliance with the DPA.

**Creating a good practice forum:** we recommend the ICO considers creating, monitoring and managing an online 'Good Practice Forum' on its web site, allowing the ICO and data controllers to disseminate good practice more widely and effectively. This 'Good Practice Forum' would be a pragmatic, proactive and cost effective method for the ICO to disseminate good practice approaches and procedures, including good practice discovered in the course of a GPA. A well-promoted and managed forum should help to minimise resource implications of disseminating good practice. This will assist in advertising an increased number of GPAs and help to dispel ideas that GPAs are an arduous undertaking for a data controller.

## Inspection powers

The DPA provides the ICO with a range of tools to support them in carrying out assessments of compliance. The ICO can issue a data controller with an Information Notice where they reasonably requires information for the purpose of determining compliance with the data protection principles, or following a request from a data subject. An Information Notice can require a data controller to provide the ICO with required information, in a specified form, to assess compliance with the data protection principles. Failure to comply with an Information Notice is a criminal offence under the DPA.

The DPA provides the ICO with powers of entry and inspection on occasions where it requires access to premises to undertake an inspection. The ICO can apply to a judge for a warrant to enter premises without consent. Before issuing a warrant the judge must be satisfied that the ICO:

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

Once on the premises the ICO can search the premises; inspect, examine, operate and test any equipment used for processing personal data; and inspect and seize any documents or other material found on the premises. Attempting to obstruct or failing to provide assistance as reasonably required is a criminal offence.

The warrant can also be used to obtain evidence of a breach of the data protection principles. The ICO is not required to give notice of its intentions to search under a warrant if they are satisfied that the case is one of urgency or where it would defeat the purpose of entry.

Given the coercive nature of the power provided under a warrant and the potential interference with ECHR rights to private life and the enjoyment of private property, judicial oversight is provided.

If operated rigorously and effectively, the framework provided by the existing powers and the proposed measures to strengthen these powers provides the ICO with appropriate and adequate tools to enforce a robust data protection and data sharing regime. We recommend the following enforcement process:

- the ICO should seek consent to a GPA if not already provided by an organisation
- the ICO issues an Information Notice where they reasonably require any information for the purpose of determining whether the data controller has complied or is complying with the data protection principles
- the ICO should consider undertaking a risk assessment or issuing an Enforcement Notice where appropriate, on the basis of information gathered under an Information Notice, reasons for an organisation to withhold consent for a GPA, and previous compliance with the DPA
- the ICO should consider using their powers of entry and inspection where there are reasonable grounds for suspecting that a data controller has or is contravening any of the data protection principles, or has committed an offence under the DPA.

**Proposal 4 - That when the ICO issues an Information Notice under section 43 of the DPA they should have the power to specify the time and place that information should be provided.**

### Responses

	<b>Proposal4</b>
<b>Yes</b>	51 (71%)
<b>No</b>	10 (14%)
<b>No answer</b>	11 (15%)

A large majority of respondents agreed with the proposal to include an explicit time limit for the manner in which information should be provided under an Information Notice. There were some concerns raised regarding reasonableness of the power to specify place where information should be provided to the ICO under an Information Notice.

Axa UK Group, along with other respondents, felt the proposal would encourage data controllers to deal more quickly and effectively with potential non-compliance that could damage a data subject.

Liberty considered the current provisions in the DPA allowed an uncooperative data controller scope to hamper and delay the work of the ICO, but that this proposal would need a set of appropriate parameters, such as during normal working hours and at a location reasonably accessible by the data controller.

### Outcome

We propose to legislate to enable the ICO to specify the time and place by which a data controller must provide information requested under an Information Notice. This means a data controller would need to carefully consider how any requested information should be provided to the ICO in order to meet the deadline. Failure to provide the requested information on or before that deadline would result in the data controller committing an offence.

In order to satisfy the concerns in relation to place we propose the ICO use the power to specify place in an appropriate and proportionate manner. We envisage an appropriate and convenient location that has been agreed between the ICO and data controller will always be preferable. The route of appeal under section 48 of the DPA for data controllers in relation to the details of an Information Notice will remain in place for these additional proposals.

**Proposal 5 - That the ICO should be able to enter a data controllers' premises under a court warrant to undertake an inspection in circumstances where:**

- a) they do not have reason to suspect non-compliance or a breach of the data protection principles**
- b) they do not have reason to suspect non-compliance or a breach of the data protection principles but have completed a risk-assessment which identifies the data controller as high-risk.**

### Responses

	<b>Proposal 5a</b>	<b>Proposal 5b</b>
<b>Yes</b>	7 (10%)	30 (42%)
<b>No</b>	59 (82%)	34 (47%)
<b>No answer</b>	6 (8%)	8 (11%)

Nearly all respondents described entry to premises without evidence as disproportionate, unreasonable and unnecessary. Several responses, including those of The National Archives and Tesco, identified entry without evidence, for any purpose, as running counter to the Hampton principles of better regulation. The Association of British Insurers, The Bar Council and The Department for the Environment, Food and Rural Affairs, had reservations that entry without evidence could place a significant and disproportionate financial and administrative burden on data controllers, potentially with little justification.

The Incorporated Society of British Advertisers highlighted that measuring risk is an inexact science and that providing such powers to the ICO suggests a presumption of guilt rather than innocence. The REaD Group Plc noted that in order for the ICO to enter premises, the ICO should have already carried out a thorough investigation that would provide evidence of non-compliance. The Association of Financial Advisers, noting that after using its current powers, the ICO should have reasonable grounds to suspect a data controller of non-compliance prior to seeking a warrant under the existing powers of entry and inspection.

There was a range of responses on risk assessments. CIFAS stated that, where there was no reason to suspect non-compliance, there should be no right of entry. This was further highlighted by The National Association of Data Protection Officers, who considered that a warrant would only be justifiable in situations where evidence of non-compliance is available, possibly accompanied by a risk assessment. Openwork UK Ltd argued that there was no clear rationale for the ICO to use its resources towards an assessment where non-compliance was not already suspected. The Department of Transport did not consider it proportionate for the ICO to seek a warrant based solely on a risk assessment.

## **Outcome**

We have considered the range of responses regarding this proposal and do not intend to proceed. We agree with concerns that this proposal would run counter to the Hampton Review, which states that by using the best evidence to programme work, regulators could reduce or maintain the appropriate administrative and financial burdens on compliant organisations. We also take on board the range of comments made regarding the level of appropriateness for a risk assessment to form the basis of a request for a warrant.

**Proposal 6 - That the ICO should have the power to require any person on the premises, where a warrant is being executed, to provide the ICO with any information required to determine whether the data controller has complied with or is complying with the data protection principles.**

### **Responses**

	<b>Proposal 6</b>
<b>Yes</b>	42 (58%)
<b>No</b>	20 (28%)
<b>No answer</b>	10 (14%)

The majority of respondents agreed with this proposal. We agree that it is important for the ICO to have access to all the information appropriate to an investigation.

### **Outcome**

We propose to legislate to enable the ICO to require any person on the premises, where a warrant is being executed, to provide the ICO with any information as appropriate to that investigation.

## Funding

Notification fees paid by data controllers' fund the data protection responsibilities of the ICO. The DPA requires every data controller who is processing personal data to notify the ICO unless they are exempt. Failure to notify is a criminal offence.

The notification fee is currently £35 per annum, per data controller and applies to all organisations that process personal information who are not currently exempt from payment of the fee. The notification fee is the same for applicable organisations regardless of their size.

**Proposal 7 - To introduce a tiered notification fee structure to ensure the extent of regulatory activity required by the ICO is reflected more accurately in the level of notification.**

### Responses

	<b>Proposal 7</b>
<b>Yes</b>	51 (71%)
<b>No</b>	15 (21%)
<b>No answer</b>	6 (8%)

A majority of respondents agreed with this proposal. There was support for increasing the level of the notification fee while maintaining a flat rate system. However, given the overwhelming support for a tiered notification fee structure, we no longer consider the flat rate scheme viable. The vast majority in favour of this proposal agreed the flat rate fee was no longer appropriate and that a tiered notification fee structure would ensure equality in the system.

### Outcome

We will legislate to change the notification fee to a tiered structure. This proposal will end the current flat rate notification fee of £35, which has not increased since 1 March 2000 when it was first introduced.<sup>6</sup> The new criteria will place the same obligation on any data controller who currently registers or who should be registered.

The criteria for the tiered notification fee structure will be based on the definition for the size of organisations adopted by the UK Government, adapted from the

---

<sup>6</sup> ICO Annual Report 2007/08, paragraph 20

European Union definition.<sup>7</sup> The definitions we plan to use are illustrated in the table below.

<b>Band</b>	<b>Turnover<sup>8</sup></b>	<b>Employee number</b>
Band A	Not more than £2,800,000	Not more than 20
Band B	Not more than £25,900,000	Not more than 250
Band C	Above £25,900,000	Above 250

We are assessing the number of tiers in the notification fee. The self-assessment process will use 'total number of full time equivalent employees and turnover' from the most recent complete financial year; both must be satisfied to allocate an organisation to a tier. Data controllers with no turnover should use their budget for the most recent financial year in place of turnover. The above criteria are objective and easy for any organisation to calculate ensuring minimal burden on business.

There are various organisations that sell and make publicly available data on turnover and employee numbers, including Companies House. We recommend the ICO use these facilities to assist in regulating the tiered notification fee structure where appropriate. Using publicly available information should minimise the resource requirements of the ICO.

We recognise the concerns of the British Retail Consortium who are opposed to any change in the fee structure that would impose higher costs for their members. However, the flat rate fee of £35 was installed in 2000 and has not been increased. Allowing for inflation<sup>9</sup> since 2000, the fee level for 2008 for all data controllers would have been £44.32. In addition, since 2000, the complexity of information technology and data processing systems has increased substantially. We do not feel an increase in the fee for larger data controllers unreasonable. However we do agree that, if at all possible, maintaining the lowest fee level in a tiered structure at the current rate is appropriate for smaller organisations.

---

<sup>7</sup> On 6 May 2003 the European Commission adopted a new Recommendation 2003/361/EC regarding the SME definition which replaced Recommendation 96/290/EC from 1 January 2005.

<sup>8</sup> The numbers relating to turnover are updated annually by BERR and those updates should be used in subsequent years.

<sup>9</sup> RP04 – Retail Price Index (all items) issued by the Office of National Statistics.

**Proposal 8 -That there should be an additional penalty, other than removal from the register, for data controllers who knowingly and deliberately provide incorrect information as part of their notification fee self assessment.**

### Responses

	<b>Proposal 8</b>
<b>Yes</b>	52 (72%)
<b>No</b>	12 (17%)
<b>No answer</b>	8 (11%)

The majority of respondents agreed with this proposal to ensure there was a penalty in place to deter falsely notifying details to the ICO.

### Outcome

We agree with the necessity to ensure that there is a sufficient penalty in place to deter notification with false details. We will consider the most appropriate way of ensuring this penalty is in place.

### Additional recommendations

**Reducing the complexity of notification:** the Capital Partnership stated that any reluctance to register was due to either, lack of awareness of the necessity to register, or awareness of the complexity of registration. We suggest the ICO considers raising the profile of the necessity to register and to reduce the complexity involved with registration where appropriate.

There were seven prosecutions for non-registration by the ICO in the financial year 2007/08<sup>10</sup>. Creating a more flexible funding regime along with a clearer system for registering should allow the ICO to invest more resource in prosecuting data controllers who do not register when required to do so. A harder line approach to non-registration will send a clear signal and increase deterrence and we recommend this course of action.

**Introducing online payment:** we recognise the ICO has committed to investigating in more flexible means of payment.<sup>11</sup> We welcome this and recommend that the ICO consider allowing payment online to help reduce the administrative burden on data controllers.

---

<sup>10</sup> ICO Annual Report 2007/08

<sup>11</sup> ICO Annual Report 2007/08

## Conclusion

The responses to our consultation and at our event have helped to assist in shaping the policy proposals as outlined above. We are grateful to all those who responded providing helpful and insightful input into the policy process.

We will work closely with the ICO to ensure any further work on these proposals is done so in accordance with our policy objective of protecting people's personal data more effectively.

We have previously signalled our intentions in May 2008 to bring forward changes in the draft legislative programme under the area of strengthening data protection laws through the audit powers of the ICO. Proposals requiring secondary legislative change will be brought as and when it is appropriate to do so.

There needs to be a framework in place that increases public trust and confidence in the handling of personal data by both the public and private sector. The measures proposed in this response complement the ICO's existing powers and ensure it has an effective and powerful range of tools to carry out its regulatory functions.

### Specific sector concerns

Concerns were raised in several sector specific areas. Several responses queried how these proposals would sit with those powers of the Financial Services Authority (FSA). In order to ensure effective and appropriate regulation and to avoid duplication of regulation, it is necessary for the ICO to continue engagement with the FSA to ensure their two regimes work effectively together ensuring the duplication of regulation is minimised or eradicated all together.

The Newspaper Society were concerned with the protection of journalistic material and the safeguarding of journalistic sources. We can confirm that any amendments, where applicable, will not nullify the protection afforded currently by the DPA, nor allow that protection to be easily bypassed.

Cheshire Constabulary raised the concerns over CCTV and how CCTV fits into the data protection framework. The Home Affairs Committee report on 'A Surveillance Society?'<sup>12</sup> recommended that the ICO lay before Parliament an annual report on surveillance and for Government to produce a response to each report to be laid before Parliament for debate. The Prime Minister in his speech on 'Security and Liberty'<sup>13</sup> accepted this recommendation and the ICO is taking this forward.

---

<sup>12</sup> The Government reply to the Fifth Report from the Home Affairs Committee Session 2007-08 HC 58 – "A Surveillance Society?"

<sup>13</sup> Prime Minister's speech: "Security and Liberty" - 17 June 2008

## Glossary

---

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

**Civil Monetary Penalty/Section 55 A-E:** when brought into force, the ICO will be able to issue a civil monetary penalty for serious breaches of the data protection principles of a kind likely to cause substantial damage or distress. It will apply in cases of deliberate breach and where a data controller is aware that there is risk of serious breach but fails to take reasonable steps to prevent such a breach.

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

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

**Enforcement notice/Section 40 notice:** is issued by the Commissioner if he is satisfied that a data controller has contravened or is contravening the data protection principles. The notice sets out the steps that the data controller must take to comply with the relevant requirements of the Act. The notice may be appealed to the Information Tribunal, which may confirm, amend or overturn it. However, in the absence of an appeal, if the data controller fails to comply with a notice a criminal offence is committed.

**Information notice/Section 43 notice:** is a written notice from the Commissioner to a data controller or a public authority seeking information that the Commissioner needs to carry out his functions. Failure to comply with an information notice is an offence.

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

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

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

**Powers of Entry and Inspection/Section 54A and Schedule 9:** enables the Commissioner to enter a data controller's premises to inspect any personal data recorded in the Schengen Information System, the Europol Information System and the Customs Information System. Section 50 gives effect to Schedule 9 of the DPA, which provides for the Commissioner to apply to a judge for a warrant to access premises without consent.

## Consultation co-ordinator contact details

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

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

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

If your complaints or comments refer to the topic covered by this paper rather than the consultation process, please direct them to the contact given on page 3.

## The consultation criteria

The six consultation criteria are as follows:

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

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

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

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

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

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

## **Annex A – List of respondents**

Acxiom Ltd

APACS/Payments Council

Axa UK Group

The Association of British Insurers

The Association of British Pharmaceutical Industry

The Association of Chief Police Officers (Scotland)

The Association of Financial Advisers

Barclays

The Bar Council

Birmingham & Solihull Mental Health Foundation Trust

The British Bankers Association

The British Computer Society

The British Retail Consortium

British Telecom

Brunel University

The Capital Partnership

Cheshire Constabulary

CIFAS

Confederation of British Industry

Coventry City Council

Credit Services Association

The Data Protection Forum

Datpro Ltd

Deloitte and Touche LLP

The Department of the Environment, Food and Rural Affairs

The Department of Transport

The Department of Work and Pensions

The Direct Marketing Association UK Ltd

The Environment Agency

Equifax

Experian

The Federation Against Software Theft

FCE Bank Plc

Friends Provident

General Medical Council

Halifax, Bank of Scotland

The Incorporated Society of British Advertisers

Information Commissioner's Office

The Institute of Chartered Accountants in England and Wales

Justice

King's College London

Leicester City Council

Leicestershire Information Management Group

Liberty

Lloyds TSB

London Borough of Richmond

LGR Information Management Group (Cheshire)

MacRoberts LLP

Medical Protection Society

Member of public

The National Archives

The National Association of Data Protection Officers

The National Association of Voluntary and Community Action

The National Information Governance Board

National Services Scotland (NHS)

Newcastle University

The Newspaper Society

Norfolk County Council

North Yorkshire County Council

Openwork Ltd

Patient Information Advisory Group

The REaD Group Plc

Royal Bank of Scotland

The Scottish Ambulance Service

Standard Life

Stockport Council

Tesco

University of Edinburgh

University of Huddersfield

University of West Scotland

University of Wolverhampton

Welsh Assembly Government

© Crown copyright  
Produced by the Ministry of Justice

Alternative format versions of this report are available on request from  
[matthew.benson@justice.gsi.gov.uk](mailto:matthew.benson@justice.gsi.gov.uk) (020 3334 3769) .