Ministry of JUSTICE

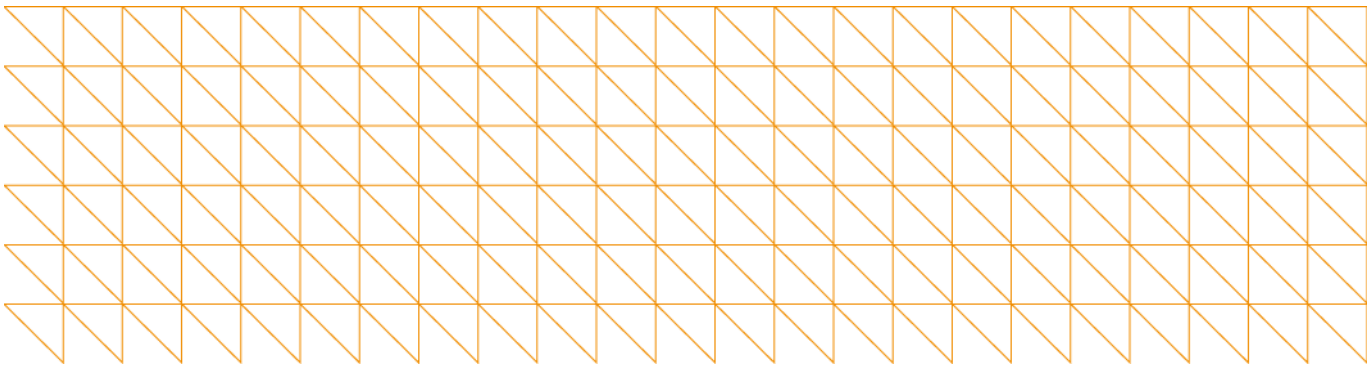
Civil Monetary Penalties- Setting the maximum penalty

Summary of responses

Response to Consultation Paper

CP(R) 48/09

12 January 2010



Ministry of JUSTICE

Civil Monetary Penalties- Setting the maximum penalty

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

About this consultation

To:	This is the response to the consultation 'Civil Monetary Penalties – Setting the maximum penalty'. The consultation was aimed at data controllers and organisations representing them in the UK.
Duration:	From 9 November 2009 to 21 December 2009
Enquiries (including requests for the paper in an alternative format) to:	Kavita Goburdhun Ministry of Justice 102 Petty France London SW1H 9AJ Tel: 020 3334 3809 Fax: 020 3334 2245 Email: Kavita.Goburdhun@justice.gsi.gov.uk

Contents

Introduction and contact details

This document is the Government's response to the consultation paper, Civil Monetary Penalties - Setting the maximum penalty.

It covers:

- the background to the consultation;
- a summary of the responses to the consultation;
- a detailed response to the specific questions raised in the consultation;
- the next steps following this consultation.

Further copies of this response and the consultation paper can be obtained by contacting **Kavita Goburdhun** at the address below:

Information Policy Division
Ministry of Justice
102 Petty France
London SW1H 9AJ

Telephone: 020 3334 3809
Email: Kavita.Goburdhun@justice.gsi.gov.uk

This response to the consultation is also available on the Ministry's website: www.justice.gov.uk.

Alternative format versions of this publication can be requested from the address above.

Background

The Data Protection Act 1998 (DPA) provides the Information Commissioner Iwith an effective framework within which he carries out his responsibilities to regulate the DPA. Nevertheless, the Government recognises that it must develop this framework where appropriate to ensure it keeps pace with technological and other advances, as well as increased public concern over information security.

Following significant losses of personal data, a number of public requests were made to introduce a criminal offence for reckless or repeated security breaches of personal data. The Government considered that a criminal offence for such breaches would be a disproportionately heavy-handed solution 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 Information Commissioner's Office (ICO). The ICO agreed with the Ministry of Justice (MoJ), that a civil penalty would be an appropriate alternative.

Consequently, Government amended the DPA, through section 144 of the Criminal Justice and Immigration Act 2008 (CJIA), to provide the Information Commissioner with a power to impose Civil Monetary Penalties (CMPs) on data controllers.

This new section of the DPA (Section 55A) provides that the Information Commissioner may serve a data controller with a monetary penalty notice if the Commissioner is satisfied that:

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

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

(c) 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.

Section 4(4) of the DPA states that "it shall be the duty of a data controller to comply with the data protection principles in relation to all personal data with respect to which he is the data controller". In

summary, the data protection principles state that personal data shall be:

- Fairly and lawfully processed;
- Processed for specific limited purposes;
- Adequate, relevant and not excessive;
- Accurate and up to date;
- Not kept for longer than is necessary;
- Processed in line with citizens' rights;
- Secure; and
- Not transferred to countries outside the European Economic Area without adequate protection.

On 9 November 2009 Government published its consultation paper entitled "Civil Monetary Penalties - Setting the maximum penalty", which set out the proposal to set the maximum penalty for CMPs at £500,000. Government believes that this amount provides for an effective deterrent for the large majority of data controllers. At the same time, the ICO consulted on its draft guidance, which addresses 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.

MoJ's consultation paper sought views from data controllers on the maximum level of the proposed penalty, but responses to the consultation were welcomed from anyone with an interest.

The consultation period closed on 21 December 2009 and this Government response summarises the responses to the consultation, including how the results of the consultation influenced the final decisions reached.

A list of respondents is set out at Annex A.

Summary of responses

1. A total of 52 responses to the consultation paper were received. Of these, 9 were from individuals, 9 from the financial sector, 8 from the legal sector and 8 from the medical sector. In addition, the ICO provided a response, as did the Federation of Small Businesses, as well as a number of local authorities and businesses. A full list of those who responded can be found at Annex A.

2. The responses were analysed to consider whether any changes to the proposal should be made, and took into account other views expressed. The consultation asked for responses to a particular question on the maximum penalty that could be imposed by the Information Commissioner. Some responses did not provide a direct answer. Where this is the case, we have attempted to interpret their comments objectively as to whether they are in favour or against the proposal, and if so, whether they consider the maximum limit to be too high or too low.

3. There was considerable support from the majority of respondents to commence the power of the Information Commissioner to impose a civil monetary penalty on data controllers who commit serious contraventions of the data protection principles as described in section 55A of the DPA. Most responses recognised the importance of personal data, the need to keep it secure, and the harm that could be caused to individuals if it is not adequately protected. Of the 52 responses, 27 supported the proposal that a penalty of up to £500,000 provides the Information Commissioner with a proportionate sanction for serious contraventions of the data protection principles. Of the remaining 25 responses, 8 considered that the proposed penalty was too low, and 9 considered that the maximum penalty was too high. The remaining 8 responses did not respond directly to the question.

4. A number of respondents noted the importance of the proportionality of the civil monetary penalty to the level of contravention. In addition, several respondents compared the maximum level of penalty with those available to other regulators, most notably the Financial Services Authority (FSA), which is able to impose an unlimited penalty, and thought that the Information Commissioner should have an equivalent power. There was also concern that some data controllers would be subject to “double jeopardy” i.e. being fined by both the FSA and the Information Commissioner for the same contravention.

5. Some respondents were concerned that larger data controllers, who have high financial turnovers, would not feel the effect of this penalty. One response suggested that a higher maximum penalty should be over £2.5 million, but only for those larger data controllers within the higher notification band, while a lower maximum of £500,000 could be applied to those organisations within the lower notification group[1].

6. Others were concerned about the nature of CMPs; some were worried about the effect this would have on smaller businesses, especially in the current economic climate, and one respondent did not think a penalty would be appropriate as many data breaches are due to a lack of resources. A response also questioned whether CMPs are compatible with the Human Rights Act 1998.

7. Another respondent considered the DPA difficult to interpret, and considered the proposed maximum penalty to be unfair. Some uncertainty was also expressed about who could receive a civil monetary penalty (one respondent suggested that CMPs would be applied to everybody, including individuals processing data for personal purposes) and in what circumstances, while another believed that a higher penalty should be applied to government departments and agencies. Some responses considered a penalty of 10% of the annual turnover of an organisation to be a more effective deterrent.

8. However, overall, there was support for the need for the Information Commissioner to have an additional power to tackle serious contraventions of the data protection principles, and, as mentioned above, a majority of the responses were in favour of a maximum penalty of £500,000.

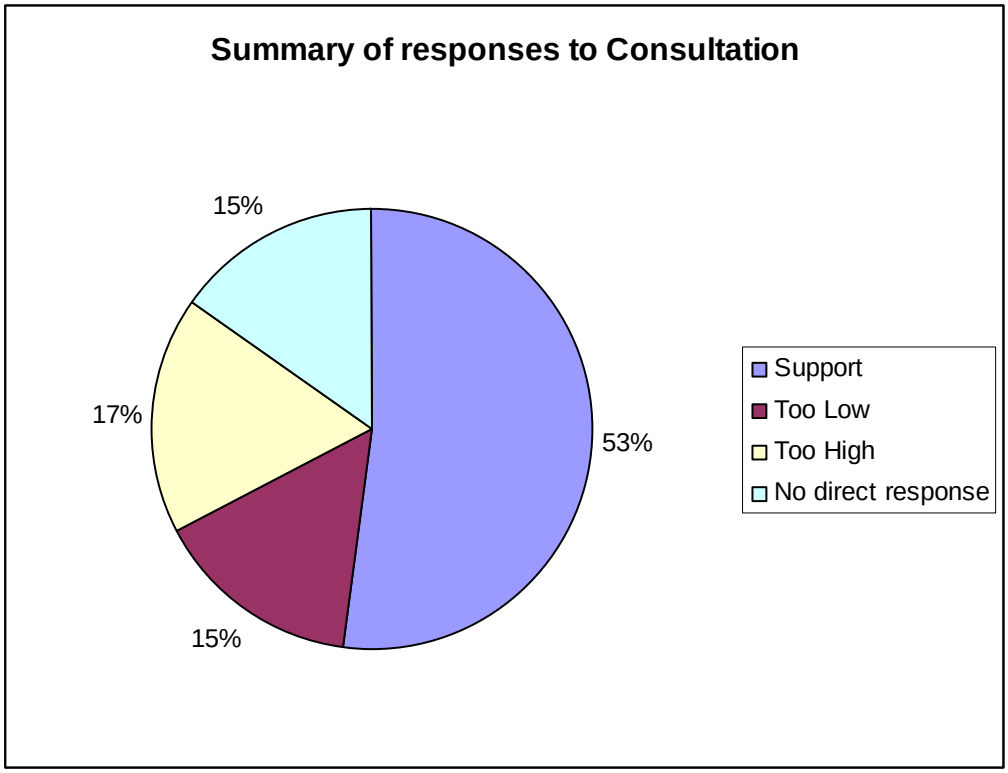
[1] Notification is the process by which a data controller gives the ICO details about their processing of personal information. Currently the notification fees are £35 for tier one and £500 for tier two data controllers; those data controllers included within tier two have a turnover of £25.9M **and** 250 or more members of staff; they may also be public authorities with 250 or more members of staff.

Responses to the question

1. **Do you consider that a penalty of up to £500,000 provides the ICO with a proportionate sanction for serious contraventions of the data protection principles?**

Yes		**27 (53%)**
No	**Too low**	**8 (15%)**
	Too high	**9 (17%)**
No direct response		**8 (15%)**

The pie chart below reflects the responses:



Conclusion and next steps

1. We welcomed all responses received. The majority of the views were in favour of the Government's proposals and supported the arguments made in the consultation paper. The Government believes that it is important to send out the right message on data protection. Most data controllers do comply with the data protection principles, which 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.

2. The Information Commissioner, as a public authority, is under an obligation to act fairly and reasonably. He is obliged by statute to produce and observe guidance on the administration of CMPs. This guidance (which was open to comments from the public during the course of MoJ's consultation) provides that the Information Commissioner will not cause undue financial hardship for data controllers as a result of the application of a penalty. Additionally, the guidance provides that the Information Commissioner will take into account the sector a data controller is in (for example, whether the data controller is a voluntary organisation), as well as the size and financial and other resources of a data controller before determining the amount of a monetary penalty. As a result of this, small companies, or those with limited financial resources, will not be placed at risk of unreasonable penalties. The proposed penalty of £500,000 is the maximum that can be applied. We do not expect the maximum penalty to be applied routinely, as this will only be relevant for the most serious cases.

3. It is important to take into account that a serious contravention will not in itself lead to a civil monetary penalty, as the DPA provides that the ICO has to be satisfied that the data controller:

    a) deliberately commits a serious contravention of the data protection principles which is likely to cause substantial damage or substantial distress; or

    b) commits a contravention of the data protection principles which is likely to cause substantial damage or substantial distress and knew or ought to have known that there was a risk that the contravention would occur and, 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.

4. The Information Commissioner's guidance on CMPs will explain the circumstances in which the Information Commissioner would consider it appropriate to issue a monetary penalty notice and how he will determine the amount of the penalty. It will provide information on how this power will be used, and what factors are likely to be taken into consideration in determining the level of penalty to be imposed and relevant interpretations. Details are likely to include the severity of contravention, number and nature of the contravention, number of data subjects involved etc. The guidance will also set out details of how a data controller can appeal against the issue and amount of a civil monetary penalty.

5. At an early stage, Government considered options for imposing a penalty based on the turnover of an organisation. However, as explained in the Impact Assessment published alongside the consultation document, there was a greater administrative burden involved in operating a turnover-based system for both the ICO and data controllers. For this reason, we consulted only on a fixed maximum penalty. As set out in the Impact Assessment, percentage of turnover was one of the indicators we used to arrive to a maximum fixed penalty of £500,000. Further details on this point are available in the annexed final Impact Assessment on CMPs.

6. The Information Commissioner's power to impose CMPs will apply to all data controllers, including government departments, private sector companies and charities. It will not apply to individuals processing personal information for the purposes of that individual's personal, family or household affairs as this is exempt from the data protection principles by section 36 of the DPA.

7. Although it is possible that both the FSA (or other regulators) and the Information Commissioner could take action against the same data controller, this is unlikely to happen. Where the statutory powers of both the Information Commissioner and other regulators allow them to intervene in the same case, both regulators will work closely to ensure that the most appropriate action is taken and that a data controller is not punished twice. The Information Commissioner's published draft guidance covers this point.

8. Many respondents compared the proposed maximum penalty with that of the FSA (which is unlimited) and believed this should be consistent. Government considered providing the Information Commissioner with a power similar to that of the FSA. However, as

section 55A (5) of the DPA provides that "the amount determined by the Commissioner must not exceed the prescribed amount" this option was discarded because the legislation requires a maximum amount to be set. For this reason, Government does not believe that the financial penalties available to the ICO should be equivalent to, or exceed those, of the FSA and other regulators.

9. Government does not agree with the suggestion that the level of complexity of the DPA makes compliance difficult. It also disagrees with the explanation that a lack of resources is the reason why many data breaches occur. Data controllers have a responsibility to ensure that the processing of personal data is done in a fair and lawful manner. As regulator of the DPA, the Information Commissioner is also responsible for promoting good practice and providing advice on compliance with the data protection principles, and the ICO's website provides much useful advice and guidance.

10. The ICO also recently published a data protection guide, which explains the purpose and effect of each principle, and gives practical examples to illustrate how the principles apply in practice. Section 55B of the DPA specifically provides data controllers with the ability to make written representations in relation to the proposed monetary penalty. This allows data controllers to produce any financial or other relevant information to the ICO to consider in finalising the amount of the potential penalty. In addition, data controllers can ask for the Information Commissioner to carry out a good practice assessment, to ensure that their data protection processes meet legislative requirements.

11. Part 5 of Schedule 20 to the Coroners and Justice Act 2009 inserted two exemptions from CMPs. These exemptions provide that the Information Commissioner cannot impose a CMP on a data controller where the information concerning a contravention has been obtained as a result of an assessment notice or an assessment under section 51(7) (good practice assessment), (for example, information about inadequate security arrangements).

12. We have considered whether the proposal is compliant with Article 6 of the European Convention of Human Rights (ECHR), and believe that civil monetary penalty scheme and its incorporated safeguards to be fully compliant.

13. We recognise that 17 of the 52 responses (32%) did not consider a penalty of up to £500,000 to be a proportionate sanction for serious contraventions of the DPA. Some believed this figure to be too high (17%), others believed it to be too low (15%), although there was no

overall consensus of what the maximum penalty should be. We considered the responses carefully, and, taking into account that a majority of responses supported the maximum penalty, Government had decided to implement its original proposal.

14. However, this policy will be reviewed within three years, when its effectiveness will be considered. It is therefore possible that the maximum penalty may be increased, or decreased at that stage. Changes to the amount can be made through secondary legislation.

15. To conclude, Government believes it is necessary to give the Information Commissioner the power to impose civil monetary penalties to address serious contraventions of the data protection principles. The ICO's guidance will set out how this power will be used, and the appeal procedures on both the application of this power and the level of penalty will provide the necessary safeguards to ensure that this power is used in a fair and proportionate manner. The Government therefore intends to take these proposals forward.

16. Alongside the publication of this consultation response, the Government is making one Statutory Instrument in Parliament, and laying another in draft for approval through the affirmative procedure. These regulations provide the detailed legislative framework necessary to bring the Information Commissioner's power to serve a monetary penalty notice on a data controller into force.

17. The Government is also publishing a final version of the Impact Assessments for these proposals incorporating comments received during the course of this consultation.

18. Depending on Parliamentary approval, Civil Monetary Penalties will come into force on 6 April 2010.

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 Julia Bradford, Ministry of Justice Consultation Co-ordinator, on 020 3334 4492, or email her at consultation@justice.gsi.gov.uk.

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

Julia Bradford
Consultation Co-ordinator
Ministry of Justice
102 Petty France
London SW1H 9AJ

If your complaints or comments refer to the topic covered by this paper rather than the consultation process, please direct them to the contact given under the introduction and contact details section of this paper at page 3.

The consultation criteria

The seven consultation criteria are as follows:

1. **When to consult** – Formal consultations should take place at a stage where there is scope to influence the policy outcome.

2. **Duration of consultation exercises** – Consultations should normally last for at least 12 weeks with consideration given to longer timescales where feasible and sensible.

3. **Clarity of scope and impac**t – Consultation documents should be clear about the consultation process, what is being proposed, the scope to influence and the expected costs and benefits of the proposals.

4. **Accessibility of consultation exercises** – Consultation exercises should be designed to be accessible to, and clearly targeted at, those people the exercise is intended to reach.

5. **The burden of consultation** – Keeping the burden of consultation to a minimum is essential if consultations are to be effective and if consultees' buy-in to the process is to be obtained.

6. **Responsiveness of consultation exercise**s – Consultation responses should be analysed carefully and clear feedback should be provided to participants following the consultation.

7. **Capacity to consult** – Officials running consultations should seek guidance in how to run an effective consultation exercise and share what they have learned from the experience.

These criteria must be reproduced within all consultation documents.

Annex A – List of respondents

Nine Private Individuals

ACXION

Association of British Insurers

Association of Chief Police Officers

Association of Chief Police Officers in Scotland

Association of HM District Judges

AXA UK

Bar Council

BCS The Chartered Institute for IT

Berrymans Lace Mawer

Bank of Ireland

Brighton and Sussex University Hospital NHS Trust

British Bankers' Association

British Standards Institution

Cambridge University Hospitals NHS Foundation Trust

CIFAS

Civil Court Users Association

Cornwall Council

Dickinson Dees LLP

Dudley Metropolitan Borough Council

Equifax

Experian

Federation of Small Businesses

Forensicrisk

General Medical Council

Hay Group

HeLEX Centre for Health, Law and Emerging Technologies at Oxford (EnCoRe Project)

Information Commissioner's Office

Legal Services Commission

Licensing Executives Society (Britain and Ireland)

Lloyds Banking Group

Macroberts LLP

Merseyside Fire and Rescue Service

National Association for Information Destruction – Europe

NHS Birmingham East and North

NHS Eastern and Coastal Kent

NHS National Services Scotland

North West Information Sharing and Security Group

Scottish Government

The Direct Marketing Association (UK) Ltd

The Medical Protection Society

The REaD Group PLC

T-Mobile

West Mercia Housing Association/Group

Produced by the Ministry of Justice

Alternative format versions of this response document are available on request from Kavita.Goburdhun@justice.gsi.gov.uk.