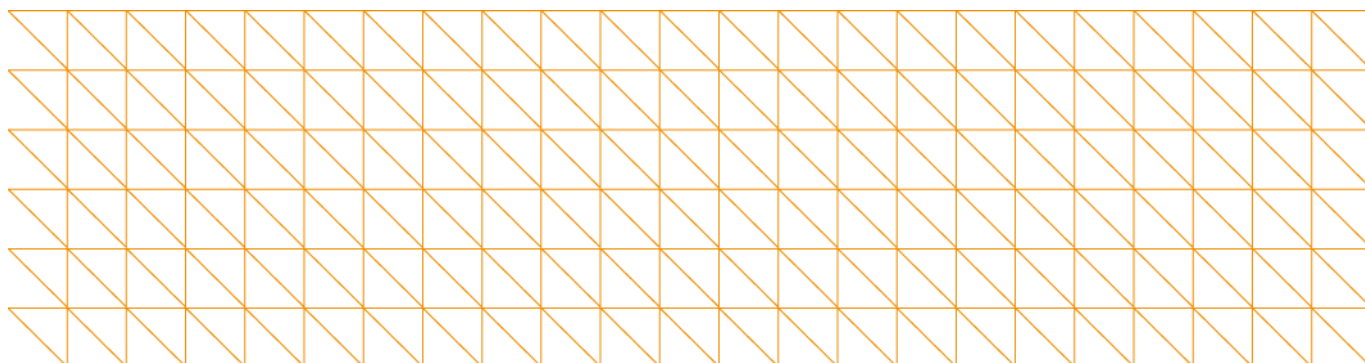


# **Call for Evidence on the Current Data Protection Legislative Framework**

## **Response to the Call for Evidence on the Current Data Protection Legislative Framework**

This response is published on 28 January 2011







Ministry of  
**JUSTICE**

## **Call for Evidence on the Current Data Protection Legislative Framework**

**Response to the Call for Evidence on the Current Data Protection Legislative Framework 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)**

## About this consultation

|                                                                                  |                                                                                                                                                                                                                                                 |
|----------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>To:</b>                                                                       | All interested parties, members of the public, organisations                                                                                                                                                                                    |
| <b>Duration:</b>                                                                 | From 06/07/10 to 06/10/10                                                                                                                                                                                                                       |
| <b>Enquiries (including requests for the paper in an alternative format) to:</b> | <p>Kavita Perry<br/>Ministry of Justice<br/>102 Petty France<br/>London SW1H 9AJ</p> <p>Tel: 020 3334 3809<br/>Fax: 020 3334 2245<br/>Email: <a href="mailto:informationrights@justice.gsi.gov.uk">informationrights@justice.gsi.gov.uk</a></p> |

## Contents

|                                                                                                                           |    |
|---------------------------------------------------------------------------------------------------------------------------|----|
| Introduction and contact details                                                                                          | 3  |
| Background                                                                                                                | 4  |
| Summary of responses                                                                                                      | 6  |
| Conclusion and next steps                                                                                                 | 21 |
| The consultation criteria                                                                                                 | 24 |
| <b>Annex A</b> – List of questions asked in the Call for Evidence on the<br>Current Data Protection Legislative Framework | 25 |
| <b>Annex B</b> - List of respondents                                                                                      | 29 |

---



## Introduction and contact details

This document is the Response to the Call for Evidence on the Current Data Protection Legislative Framework.

It will cover:

- the background to the Call for Evidence;
- a summary of some of the responses received to the Call for Evidence; and
- details of the next steps.

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

**Kavita Perry**  
**Ministry of Justice**  
**102 Petty France**  
**London SW1H 9AJ**

**Telephone: 0203 334 3809**  
**Email: [informationrights@justice.gsi.gov.uk](mailto:informationrights@justice.gsi.gov.uk)**

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

Alternative format versions of this publication can be requested from [informationrights@justice.gsi.gov.uk](mailto:informationrights@justice.gsi.gov.uk).

## Background

The Data Protection Act 1998 (DPA), transposes the EU Data Protection Directive 95/46/EC (“the Directive”) into UK law. Negotiated in the 1990s, there have been calls in recent years for a review of the Directive and for a new EU data protection instrument.

On 18 March 2010, the European Commission announced its intention to produce a proposal for a comprehensive data protection legislative framework. On 4 November the Commission published a Communication, which outlined the challenges facing the existing EU data protection legislative framework and its key objectives for a comprehensive approach to personal data protection.

The Commission’s Communication is intended to serve as a basis for further discussions between the Commission, other European Institutions and interested parties with a view to developing a new data protection legislative framework. The Commission’s draft proposal is likely to be published in mid 2011.

In preparation for this proposal, and the forthcoming negotiations on a revised EU legal instrument for data protection, the UK launched its Call for Evidence on the current Data Protection Legislative Framework on 6 July 2010. It sought information from organisations, businesses, individuals, the public sector, charities and other interested parties about the current law on data protection, especially on areas that were considered to be working well, and also those that were thought to be working not so well.

The Call for Evidence sought specific contributions on the areas listed below, and also welcomed evidence on other areas of the data protection legislative framework:

- definitions;
- data subjects’ rights;
- obligations of data controllers;
- powers and penalties of the Information Commissioner;
- the value of a principle-based approach;
- exemptions under the DPA; and
- international transfers.

In order to obtain as wide a range of evidence as possible and to support the Call for Evidence written exercise, the Ministry of Justice (MoJ) held a number of workshops for interested parties. These included representatives from the private and public sectors, as well as civil liberties groups.

At the same time as conducting the Call for Evidence, the Government published a provisional Post-Implementation Review (PIR) of the DPA, which aimed to assess its costs and benefits. The Impact Assessment accompanying the Call for Evidence has been updated to take account of evidence provided by respondents

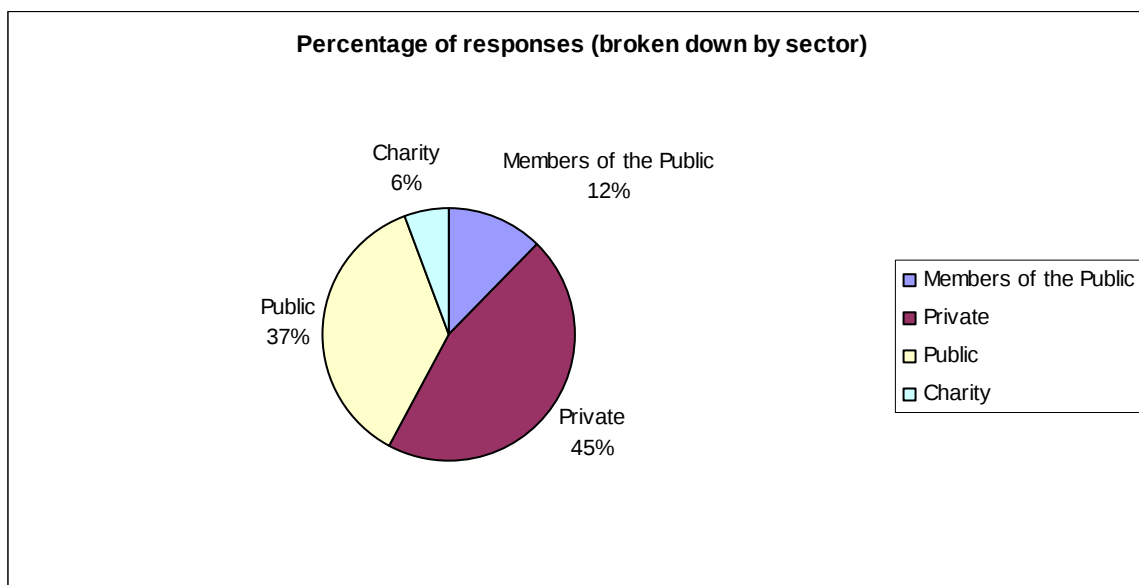
during the Call for Evidence process. This is annexed to this response document. Although this has the primary purpose of performing post-legislative scrutiny of the DPA, the findings of the PIR will contribute to the UK's overall evidence base for negotiations on a revised EU legal instrument.

The Call for Evidence closed on 6 October. This report summarises some of the main responses provided during the Call for Evidence written exercise, and expressed during the workshops, and sets out the Government's next steps.

A list of the questions asked in the Call for Evidence is at Annex A and a list of respondents can be found at Annex B.

## Summary of responses

1. A total of 163 responses to the Call for Evidence were received. The respondents included individuals as well as a range of organisations from the public, private and third sectors. A sector specific breakdown of responses can be found in the chart below:



2. A further breakdown of responses can be found below:

| Category                                                                                        | Number of Responses |
|-------------------------------------------------------------------------------------------------|---------------------|
| Education                                                                                       | 6                   |
| Expert (Information Rights)                                                                     | 3                   |
| Financial                                                                                       | 20                  |
| Government Department                                                                           | 7                   |
| Health                                                                                          | 19                  |
| IT                                                                                              | 10                  |
| Legal                                                                                           | 15                  |
| Local Government                                                                                | 8                   |
| Media                                                                                           | 11                  |
| Members of the Public                                                                           | 20                  |
| NDPB                                                                                            | 8                   |
| Other (includes Children's interest groups, Consumer groups and other businesses and charities) | 10                  |
| Police                                                                                          | 7                   |
| Retail                                                                                          | 2                   |
| Small and Medium Enterprises                                                                    | 6                   |
| Telecoms                                                                                        | 5                   |
| Trade Union                                                                                     | 2                   |
| Utility                                                                                         | 4                   |

3. There were many views expressed on different elements of the data protection framework. However, it should be stressed that not all responses provided evidence on all aspects of the questionnaire, and while some responses provided evidence, others provided views with very little supporting evidence. Where possible, we have tried to provide a quantitative idea of some of the views expressed, but these do not necessarily reflect the level and strength of the evidence provided.

## **General**

4. There was a wide range of general responses about the current data protection legislative framework. The majority of respondents, including some members of the public, thought that the current framework was generally sound, partly due to the fact that the legislation was technology neutral, which meant that amendments were not regularly required.
5. However, a smaller number of respondents from the public and private sector, as well as a number of members of the public thought that the legal framework was weak and ineffective. Particular concerns included issues such as the transfer of personal data to third parties, the treatment of medical information and the “opt out” approach to gaining consent as opposed to the “opt in” approach.
6. Other respondents thought that the DPA was too restrictive, and too complex, as well as overly bureaucratic and prescriptive, leaving data controllers with too little discretion to take account of their particular circumstances.
7. Some respondents also took the opportunity to consider the legislative framework in light of technological changes over the last few years, such as the growth of the internet, the wide uptake of social networking sites and the increase in the use of biometric information. Many thought that the legal framework should address the issues that these technologies presented, including the fact that it was easier to share personal data now than when the Directive had been negotiated.

## **Definitions**

### *Personal data*

8. Section 1 of the DPA defines personal data as those “*which relate to a living individual who can be identified – (a) from those data, or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual*”.
9. Responses to the question about the definition of personal data revealed that the definition mattered greatly, as a lack of clarity could mean that certain information may not be treated as personal data, and could therefore lead to

enforcement proceedings being issued by the Information Commissioner. A small number of organisations thought that the definition was clear and adequate, and worked perfectly well for their purposes. However, over 70% of those who provided evidence on the definition of personal data expressed the view that the definition needed to be clarified. There were uncertainties about how far other information could be defined as personal data, such as buildings (in relation to its owner), details of energy meter numbers, and energy consumption. A small number of respondents mentioned the debate on IP addresses, and the uncertainty they faced when trying to determine whether this should fall within the definition of personal data.

10. Some respondents also expressed confusion about how anonymised data fitted within the definition of personal data. With the advancement of technology and the availability of information, anonymisation of data was considered almost impossible by some. In addition, it was thought impracticable to predict what information was likely to be obtained by data controllers, which is an element that needs to be considered when determining whether specific data is defined as personal data.
11. A few respondents thought that the definition should be widened to include the data of those who were deceased, especially as some of this information, such as medical records, could be quite sensitive for members of their family. However, there were concerns about this from others. It was also clear from the views expressed that there were further complications due to conflicting opinions about the definition of personal data. A number of responses quoted the “Durant” case, in which the Court of Appeal concluded that not all information retrieved from a computer search against an individual’s name or unique identifier should be classified as “personal data”, thereby narrowing the definition of “personal data”. A number of respondents also mentioned the later House of Lords judgement in the case of *CSA v Scottish Information Commissioner*. In this case, the Court ruled in 2008 that even when data is anonymised, it can still be classified as personal data. Some respondents thought that the outcome of these two cases raised further confusion about the definition of personal data, and that this should be clarified.

#### *Sensitive Personal Data*

12. Section 2 of the DPA defines sensitive personal data as “*personal data consisting of information as to – (a) the racial or ethnic origin of the data subject, (b) his political opinions, (c) his religious beliefs or other beliefs of a similar nature, (d) whether he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992, (e) his physical or mental health or condition, (f) his sexual life, (g) the commission or alleged commission by him of any offence, or (h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.*”
13. In the opinion of some respondents, the advancements made in technology had led to uncertainties about whether certain other data should be treated as “sensitive personal data” given that it is increasingly being used as a method of

identification. More than half of those who responded on this issue felt that some biometric information should be included within the definition of sensitive personal data, as an individual's race (and possibly religion) could be determined from this information.

14. By contrast, fewer respondents made the point that not all biometric information should automatically be treated as sensitive, and that the emphasis should be the context in which the data is being processed. For example, some respondents thought that in certain circumstances biometric data was no different from photographic data in terms of identity. However, in other situations, the same data could be used to determine health issues, for example, whether a person was prone to a particular disease.
15. Just under 60% of respondents addressed the question about whether other information should be included within the definition of sensitive personal data. Of those responses, about a third maintained that any information that could be used to an individual's disadvantage, including financial, payroll and credit, should be included within the definition of sensitive personal data. A number of respondents thought, given the risk of identity fraud, financial information should be processed with a higher degree of security than other types of personal data. However, a slightly smaller number of those responses, which included those from the financial sector, thought that financial (including credit) information should not be included within the definition, because this would have a detrimental effect on consumers and small businesses' ability to obtain credit and other services. They also thought this would be burdensome for data controllers because they would have to meet additional conditions for processing such data.

#### *Data Controller and Data Processor*

16. The Call for Evidence also received a number of comments in relation to the definition of "data controller" and "data processor". "Data Controller" is defined in the DPA as "*a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed*". "Data Processor" means "*any person (other than an employee of the data controller) who processes the data on behalf of the data controller*".
17. Just over 60% of respondents replied to the question about whether the definitions of "data controller" and "data processor" as set out in the DPA and the Directive have led to confusion or misunderstandings over responsibilities. Many respondents thought that this distinction was important, as it ultimately determined who was legally responsible for the data processed. Of those responses, two thirds thought that the definitions of "data controller" and "data processor" were unclear and misunderstood, and they considered that the distinction between the two roles were unclear. Several responses raised concerns that some data processors were perceived to have very limited legal obligations under the DPA which, in their view, weakened the rights of data subjects. However, others revealed that, in practice, detailed responsibilities tended to be clarified in respective contracts where the processing of personal

data was outsourced; there were therefore advantages in having this distinction, especially in IT contracts. The definition was also helpful in knowing which body to go to in the event of a complaint. Only around 10% of responses to this question thought that the current distinctions were clear.

18. Just over 40% of respondents provided evidence on whether a separation of roles had assisted in establishing responsibilities amongst parties handling personal data. There was a mixed response to this. The majority of respondents, from members of the public, private and public sectors, considered that the separation of roles had assisted in establishing responsibilities amongst parties handling personal data. Others thought that a separation of roles was not required, and that the current distinction should be abolished. They also supported the view that a consistent and uniform level of obligation should be imposed on all organisations that hold and process personal data, regardless of whether they are a data controller or data processor. Some responses also supported the accountability principle. This promoted self-regulation, and required data controllers to implement appropriate and effective measures to ensure the principles and obligations of the Data Protection Directive were observed. Under the accountability principle, data controllers would be required to demonstrate this upon request. It would also mean that there was minimal oversight by the data protection regulator.
19. Of those respondents who wanted to retain the separation of roles, some thought that it would be beneficial if legislation clarified the definitions, supplemented by detailed guidance from the Information Commissioner's Office (ICO). It was also thought that definitions or guidance on other roles, such as "joint controllers" or "controllers in common" would be helpful.

## **Data Subjects' Rights**

### *Compliance with Subject Access Requests*

20. Section 7 of the DPA gives individuals who are the subject of personal data a general right to request access to the personal data which relates to them; this is called a subject access request (SAR). Under this section, an individual is entitled to be told by the data controller whether they or someone else on their behalf is processing that individuals' personal data, and if so, to be given a description of:
  - the personal data;
  - the purposes for which they are being processed; and
  - those to whom they are or may be disclosed.

Subject to a number of exemptions listed in the DPA, the data controller has an obligation to provide the information in permanent form.

21. Most data controllers indicated that they took their responsibility for complying with subject access requests seriously, which was evidenced in a number of ways. Some organisations had “in-house specialists” and had developed specific processes and procedures to deal with SARs. Other data controllers monitored compliance, to ensure that these requests were being dealt with in a timely manner, and kept a log so they could see how many complaints were received. However, a very small number of the public did not think that data controllers were fully complying with this obligation as they did not receive all their data when requested. Evidence also indicated that despite processing personal data, if an organisation defined themselves as a data processor, then they were not legally obliged to comply with SARs.
22. Evidence received in response to the Call for Evidence indicated that just under 30% of complaints made to the ICO were about SARs being refused. This was due to a number of reasons, such as the withholding of information under one of the grounds under Part IV of the DPA (exemptions) and the release of information about other individuals. There was also confusion about whether certain information could be classified as personal data. Evidence also revealed that some organisations are not aware of the individuals’ right of subject access.

### *Burdens*

23. The majority of responses who responded to the question on whether compliance with SARs were a burden on data controllers indicated that over the last few years there had been an increase in the numbers received, which meant an increase in burden for them. This was a concern from data controllers across the private and public sectors and across a wide range of organisations including those in health, finance and law. Some data controllers perceived this rise as a misuse of the right. For example, a number of data controllers reported that they believed that data subjects and their legal representatives were using SARs as a quick and cheap way of obtaining information for specific purposes, such as in the context of court cases, grievances and disciplinary procedures. One data controller specifically indicated that SARs were being used as an alternative way of obtaining information which would otherwise have been sent to data subjects or their representatives much later in the legal process.
24. On the other hand, some data controllers revealed that requests were for specific information, and could be dealt with promptly, and certainly within the legislative time limit of 40 days. Some stated they received requests seeking extensive data, or all data held on a data subject, which would be resource intensive. It was generally acknowledged by responses that the increase in receipt of SARs by data controllers was partly due to individuals being more aware of their rights.

25. It was also reported that much of the burden on organisations in dealing with SARs was not only in locating the information requested, but also the expense of redacting the relevant information from multiple audio, video and digital data sources. One response indicated that they were required, by legislation, to retain personal data for a specific period, which further increased the burdens placed on them by SARs.

### *Technology*

26. Views about whether technology had assisted in the compliance with SARs differed. Some responses indicated that changes in technology had made it more difficult to comply with SARs because it not only enabled personal data to be held on a number of different systems within an organisation, but also increased the amount of personal data held. In addition, some technology did not allow for individual names to be picked up from the many documents and emails that were created and processed. However, other responses indicated that technology has made it easier for them to undertake searches on their systems which meant that compliance with SARs was easier.

### *Subject Access Fee*

27. Some responses acknowledged that the charging regime for SARs was not intended as a means to recover the costs of dealing and complying with the request. Nevertheless, it was clear from the majority of responses that the costs in complying with some SARs vastly exceeded the fee that was paid by data subjects for their data, especially for the larger and more complex requests.
28. The fee for a SAR is generally fixed at £10 by the DPA, but in certain circumstances a maximum of £50 can be charged, for example, for health or educational records. Another exception to the £10 fee is in relation to bodies solely requesting details of the subject's financial status, who may only be charged a maximum of £2. Estimates from data controllers regarding the costs of dealing with a SAR ranged from £10 to over £50,000 for the more complex cases, which could take months to complete. However, it was acknowledged by many organisations that individuals were entitled to know what information was held about them, and that a modest fee should remain if it was effective in deterring frivolous requests.
29. Fewer than 50% of respondents provided a view about whether the £10 fee should be raised or lowered. The majority of those respondents thought that there should be an increase in the minimum fee (with support from one member of the public). This was the view from data controllers across both the public and private sector. Less than 15% of those responses suggested the fee should be reduced or abolished. However, there was recognition amongst respondents that a substantial fee increase should not be imposed because it would provide an obstacle for individuals to exercise their legitimate rights. In recognition of data subjects' rights, some data controllers stated in their

response that they did not charge individuals a fee for SARs, although it was noted that the £10 fee was considered too small to be worth collecting.

30. On the most appropriate level of fee for SARs, some respondents thought that a flat fee of £10 was suitable and fair, especially for those on low incomes, and should therefore remain, while others thought the minimum fee should be increased to £20 or £50.
31. Another suggestion favoured by some respondents to address the costs issue was to introduce a fixed point regime, similar to that already in force for Freedom of Information cases. The Freedom of Information Act 2000 (FOIA) provides for public authorities to either charge for or decline requests for information that would cost a public authority either more than £600 for central government or £450 for other public authorities to deal with the request, using £25 as the standard hourly rate to calculate the staff costs. This is referred to as the appropriate limit, but is limited to a number of activities that the authority can reasonably be expected to incur in:
- **determining** whether it holds the information requested;
  - **locating** the information or documents containing the information;
  - **retrieving** such information or documents;
  - **extracting** the information from the document containing it.

Some respondents thought that the more information that was requested by a data subject, the higher the fee should be. However, some respondents were concerned that the introduction of such a system to deal with costs of a SAR would be difficult to administer and would add another layer to the administration process, thereby incurring additional costs while complying with their legal obligations.

#### *Vexatious, frivolous and repetitive requests*

32. The responses revealed that not many organisations received a high level of vexatious requests, although some respondents stated that there was not a clear definition of “vexatious request”. It was acknowledged that there is no legislative basis to refuse a SAR on the basis that it is vexatious, although it was noted that there is provision for a request to be refused on the basis of disproportionate effort in certain circumstances, or on the basis that the information had recently been provided.
33. A significant number of responses reported receiving frivolous or repetitive requests for information, but most of these seemed to be “fishing expeditions”, an attempt to find out exactly what information was held in relation to a particular individual. Those data controllers indicated that they complied with those types of requests, even though the DPA was clear that such requests did not need to be complied with unless a reasonable interval had elapsed between compliance with a previous request and the making of a new one. Some data controllers indicated that they refused the request if circumstances

had not changed since the previous request, or they only provided additional (new) information if appropriate.

#### *Other Rights under the DPA*

34. The DPA provides a number of other rights for data subjects:

- section 10 relates to the right to prevent processing likely to cause damage or distress;
- section 11 is the right to prevent processing for purposes of direct marketing;
- section 12 relates to rights in relation to automated decision-taking;
- section 13 entitles a data subject to compensation where damage has been suffered by reason of any contravention by a data controller of the requirements of the DPA; and
- section 14 addresses rectification, blocking, erasure and destruction of a data subject's personal data.

35. Although these rights were acknowledged as important by many data controllers, most responses indicated that, with the exception of the right to opt out of direct marketing (section 11), the other rights under the DPA were used infrequently. Some respondents were of the opinion that sections 13 and 14 were rarely used as these placed a heavy burden on data subjects to take a data controller to court. But responses were clear that these rights were important in trying to achieve redress against data controllers.

#### *Strengthening Rights under the DPA*

36. Although some responses suggested that individuals' rights did not need to be strengthened, it was acknowledged that there is a need for better education about these rights. A number of concerns were expressed about the obligations that these rights imposed on data subjects.

37. Some respondents thought the burden on data subjects to instigate legal action against a data controller was unfair, and that the onus should be placed on the data controller to rectify any damage done. Those respondents were of the view that individuals should be compensated for any genuine harm they suffer.

38. A number of respondents considered that section 13 was unfair to data subjects in that it only provided for compensation for "damage" when in fact "distress" can also be demonstrated, or where the distress caused is by processing of personal data for the "special purposes" (defined in Section 3 of the DPA as the purposes of journalism, artistic purposes and literary purposes). Respondents also thought that allowing the ICO to investigate claims under sections 13 and 14 of the DPA and to order compensation or rectification,

rather than the data subject having to have recourse to litigation, would strengthen individuals' rights.

39. Some respondents also thought that the rights under sections 10 and 12 could be clarified, although it was noted that the number of applications made under section 10 to data controllers had increased over the last few years. It was also considered by a small number of respondents that given data subjects had to prove that the processing of data is causing or is likely to cause substantial damage or substantial distress to them or to another person under section 10, guidance on how this could be substantiated would be helpful, to both data controllers and data subjects. There was a general feeling that rights under section 12 were rarely used.

## **Obligations of Data Controllers**

### *Data Breach Notification*

40. Just under 66% of responses received commented on whether there should be mandatory breach legislation. Around three quarters of those responses did not think that such legislation should be introduced. Some data controllers thought that ICO guidance about when data subjects should be notified of a breach was suitable, although other organisations stated that they had their own processes and criteria in place which would determine when individuals and the regulator should be notified. Most data controllers thought that notification should be undertaken proportionately, and therefore should only take place in certain situations, for example, depending on the scale of the breach, the type of data lost and the risk of harm to data subjects.
41. It was acknowledged by many data controllers that mandatory notification would be burdensome, both to them and also to the ICO, therefore notification should be restricted to the most serious situations. Most respondents thought that this should be a matter for the data controller to decide when notification should take place, based on the possible harm that could be caused. Some responses cited evidence from the United States which suggests that mandatory notification does lead to "notification fatigue" where, over time, data subjects do not take any notice of data breaches, including those of a serious nature. However, other respondents thought that data subjects had a right to know when their personal data had been compromised so they could take appropriate action to protect themselves against possible harm caused by the data breach, such as identity theft.
42. Respondents had difficulty in quantifying the costs for mandatory breach notification. Many data controllers stated that the work involved would depend on the type of data breach and could include a number of different costs including communication, drafting and sending of notices, legal counsel, data protection experts, and establishing help lines.
43. The responses received indicated that very few data controllers were routinely notifying data subjects where there had been a breach of data security. Most responses indicated that this was done only where there was a chance of significant harm being caused to the data subject.

### *Exemptions from Registering with the Information Commissioner*

44. Section 17 of the DPA requires every organisation that processes personal data to notify the ICO of that processing unless they are exempt. Data controllers are therefore required to inform the ICO of certain details about their processing of personal data, which is published on a public register. The main purpose of notification is to promote openness in the use of personal data.
45. Although many respondents thought that the current exemptions strike the right balance between reducing burdens and transparent processing, other responses indicated otherwise. There were some suggestions about broadening the current exemptions for more routine processing, such as processing for statutory functions. It was also suggested by some respondents that an exemption should exist for the processing of personal data for both “research” and “journalism, literature and art” as well as for personal data held by an archives service for archival preservation.
46. On the wider point of notification, many data controllers thought that the current registration process was complex and too onerous and they would welcome a simpler process which was standardised across Europe. Some respondents thought that notification should be abolished on the basis that it served no apparent purpose apart from generating funds for the ICO. Others failed to see the benefits that registration achieved for businesses. One response suggested exempting small and medium-sized companies from notification.

### **Powers and Penalties of the Information Commissioner**

#### *Adequate Powers*

47. About 25% of responses answered the question of whether they thought the Information Commissioner had adequate powers to enable him to carry out his duties. Of those responses, just over 50% thought that the ICO had adequate powers. These respondents were both private sector and public sector data controllers, from a wide range of areas including health and retail. It was generally accepted that the new power to impose a civil monetary penalty of up to £500,000 would serve as a successful deterrent to data controllers who do not take their data protection responsibilities seriously, although some thought that this power should also be extended to data processors. A small number (around 4% of respondents) thought that time should be allowed to review how this new power worked in practice before considering any additional powers for the ICO.
48. Around 45% of respondents thought that the ICO did not have sufficient powers, and this includes most members of the public who provided a response in this area. Some of these expressed concern that the maximum financial penalty for a serious breach of the data protection principles was not as high as that which could be imposed by the Financial Services Authority or the Competition Commission. One response examined the recent case

involving the trade in personal data where almost £500,000 was paid for personal information, sometimes consisting of sensitive personal data, but the convicted data controller was only fined £5,000 (plus costs).

49. Responses revealed a wide range of support for the introduction of custodial offences for both serious breaches of the DPA and the unlawful obtaining of personal data. Many believed that this should only be used in the most extreme cases, although there was opposition to the introduction of custodial sentences by a number of media organisations.

#### *Further powers*

50. Some respondents thought that the remit of the ICO should be extended to cover other legislation that interacts with the DPA, such as the Human Rights Act 1998. However, it was acknowledged that decisions taken by the courts and tribunals in relation to DPA cases took other legal requirements into account.
51. Others thought that the ICO should have the power to undertake unannounced audits on all data controllers (not just Government departments), and that it should be able to regulate data processors as well as data controllers. In addition, one respondent suggested that the ICO should be able to ban directors and senior managers from holding directorships.
52. A number of responses commented on the resources available to the ICO, and thought that more should be made available, to allow the follow up and investigation of more cases. Some responses also suggested that prompt investigation might have prevented further data breaches.

#### **The principle-based approach**

##### *Is the principle-based approach correct?*

53. Some data controllers welcomed the principle-based approach on the basis that it is technologically neutral, and therefore applicable in a wide variety of situations and sufficiently “future-proofed”. However, a number of other respondents maintained that this flexible approach gave rise to a number of issues concerning interpretation, and a number of respondents thought that the principles needed to be supported by detailed guidance by the ICO to assist in implementation. For example, the principle on retention (the fifth data protection principle) did not provide additional details on what was an acceptable period to retain personal data in certain circumstances. Given technological advancements, it was considered that additional guidance could be helpful in meeting the seventh data protection principle which required appropriate technical and organisational measures by data controllers to protect personal data.
54. Some respondents referred to an accountability principle, a proposal put forward by the Article 29 Working Party. The Working Party viewed this as a way to allow each organisation to develop its own self regulation methods and best practice to ensure they are compliant with the DPA. As stated in their

Opinion, *“In a nutshell, a statutory accountability principle would explicitly require data controllers to implement appropriate and effective measures to put into effect the principles and obligations of the Directive and demonstrate this on request. In practice, this should translate into scalable programs aiming at implementing the existing data protection principles...”*. Data Controllers would therefore be responsible for ensuring that they take a strategic, risk-based approach when determining effective and appropriate measures based on the nature and risks of the personal information being processed.

## *Consent*

55. There were mixed views about whether the current consent condition is adequate. The majority of responses stated that there was a great deal of uncertainty about how consent works as part of the fair and lawful principle, which was further complicated by the lack of a definition of consent in the DPA (although it is defined in the EU Data Protection Directive).
56. Some responses stated that consent was obtained if data subjects were fully informed and aware of what they were consenting to. Many respondents thought that clearer guidance from the ICO would be helpful in understanding how to obtain consent appropriately, especially if such guidance was targeted towards certain disciplines such as employment, medicine, research and adoption.
57. Where consent was sought, it was usually done on an individual basis, specifically for processing for particular purposes. A number of respondents thought that “consent” did not need to be defined within the DPA because a definition already existed in the Directive. This states that “the data subject’s consent shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.” However, some respondents thought that this definition was too restrictive, and there was concern that there would be serious implications in those situations where consent could not be freely given, for example, by an unconscious patient.
58. Some data controllers thought that any moves to make the consent conditions more onerous, or more explicit (for example, by requiring a signature or ticked declaration every time personal data was processed) would have a significant impact on business. However, many data controllers acknowledged that it was important to provide sufficient information to data subjects to enable them to understand how their data would be processed. It was also pointed out that consent was only one of a number of conditions required to enable processing to be fair and lawful, and that data controllers could use one of the other conditions if it was considered to be more applicable.
59. It was generally agreed that fair processing notices were a way for data subjects to see how their information is being used and shared. However, many data controllers did not know whether they were actually read by data subjects prior to providing consent (if this was sought), although some organisations received follow-up questions on their fair processing notice which indicated that it was being read by some people. It was generally thought that

data subjects did not read such notices in detail, usually because they are long and difficult to understand. Evidence suggested that using simple plain language or placing fair-processing notices at the top of forms could encourage data subjects to read them.

### **Exemptions under the Data Protection Act 1998.**

60. There was a wide range of views over whether the current exemptions were adequate. The majority of respondents who provided evidence thought that the exemptions were not working well and some provided suggestions for new exemptions. There were specific examples of confusion over how these exemptions operated. For example, some responses from both the private and public sector reported that the section 29 exemption in relation to personal data processed for crime and taxation was relied on too frequently and tended to be used routinely by organisations such as law and other enforcement authorities.
61. Confusion was also expressed about how this exemption interacted with other legislation, such as the Human Rights Act 1998 and the law of confidentiality, as well as EU legislative requirements in relation to anti-money laundering and anti-fraud requirements. Confusion over processing sensitive personal data under section 29 and section 35 (legal proceedings) was also noted.
62. Responses also included views on section 30 (exemptions relating to health, education and social work) which some thought were confusing and unfair to pupils because it meant that sensitive educational and medical information could be divulged by the school to the parents of the pupil. It was also considered by a few respondents that clarification was needed over how the exemption in section 33 (research, history and statistics) interacted with the processing of sensitive personal data, as there seemed to be confusion over the interpretation of the current exemption from the requirement for consent for medical research.
63. In terms of including new exemptions within the DPA, some responses suggested that a specific exemption could be added in relation to information sharing where the purpose was to safeguard vulnerable adults and children. It was also noted that the widespread use of social networking media needed to be considered in the context of the “domestic purposes” exemption in section 36 of the DPA.
64. Many media organisations responded that the current exemptions concerning the processing of personal data carried out solely for journalistic purposes should be strengthened to improve access to information for journalistic purposes and to safeguard freedom of expression. Some of the other responses called for guidance on exemptions for use in specific circumstances, for example in connection with adoption and fostering, and for historical research purposes. Concerns were also raised by a number of medical and statistical bodies about how the requirement to obtain consent from data subjects for personal data, such as medical information, affected their ability to undertake research, especially where this involved the secondary use of data.

## **International Transfers**

65. Some data controllers revealed that in certain situations (i.e. one-off data sharing arrangements) using model contract clauses was very helpful and they provided a convenient way to comply with the eighth data protection principle. However, the majority of responses suggested that the use of these clauses for complex data transfers was often difficult, and burdensome, and not suitable for the transmission of large data flows in a globalised world.
66. Respondents said that recent rapid technological changes made many of the traditional methods of transferring personal data outdated. Services such as cloud computing often make geographic boundaries around data sharing irrelevant and the increased use of email and the internet for transactions could make it difficult to determine when a transfer of personal data was taking place. The general view was that improvements were required to make the system for international transfers simpler and clearer for both data controllers and data subjects.
67. Some responses remarked that relatively few countries had been found by the European Commission to be 'adequate' for the purpose of international transfers and called for both more effort in assessing other countries as 'adequate' and simplification of the process. Similarly, respondents said that only a limited number of companies had signed up to the US Safe Harbor provisions, which also restricted transfers. Some of the respondents suggested that the current restrictions on transfers outside the EEA should be removed and a more globalised approach be adopted. Another option put forward was to introduce a risk-based approach to ensure the implementation of appropriate security measures for the data being processed. It was suggested that this requirement could mirror those recently introduced into the review of the ePrivacy Directive.

## Conclusion and next steps

1. The Call for Evidence has been a useful exercise to gather a wide range of views on the current legislative framework for data protection. It highlighted a number of key issues and practical matters that the Government will take account of. These included the need to negotiate for a legislative framework that is flexible and adaptable but also clear and robust; that takes account of future technological changes; and is not disproportionately burdensome on data controllers.
2. Responses to the Call for Evidence confirmed that technology made all aspects of personal data processing dramatically easier, from overseas transfers to archiving. Increases in technologies, such as cloud computing and social networking sites, have raised new data protection and broader privacy issues. With technology continuously evolving, respondents were clear about the importance of “future proofing” the new data protection legislation.
3. There were also concerns from respondents about how the data protection framework interacts with other legislation and requirements, such as the Human Rights Act and obligations relating to money laundering. A number of respondents also compared the Data Protection Act to the Freedom of Information Act, and thought the two regimes should be more closely aligned.
4. Some new ideas and principles were also discussed as part of this exercise, including the “accountability” principle, a proposal put forward by the Article 29 Working Party, which was commonly seen as a way of strengthening the role of the data controller and increasing their responsibility.
5. As noted earlier in this paper, the European Commission published a Communication on “A comprehensive approach on personal data protection in the European Union” on 4 November, after the Call for Evidence had closed and the Government responded to the Commission’s consultation on the Communication on 14 January. This response supported many of the Commission’s views, but recognised that some of the more far-reaching proposals would need to be carefully assessed to determine the benefits for data subjects and the impact on data controllers. For example, the Government supported the Commission’s intention to look at how best to strengthen individuals’ rights and enhance their control of their data so data subjects might be better informed about how, why, by whom and for how long their data is collected and used; there was also support for this from some of the respondents to the Call for Evidence. However, some of the Commission’s proposals could involve considerable costs and a variety of practical implications might arise for data controllers, so these issues will need to be looked at carefully.
6. As this work progresses, the Government will consider proposals in light of two main objectives: protecting individuals’ privacy and respecting their rights, and ensuring the burden on data controllers is not disproportionate. The

Government also believes that resource implications for businesses, particularly small and medium sized entities, must be proportionate to the benefits achieved by increased safeguards. In addition, the Coalition Government is firmly committed to protecting the security of its citizens and restoring and defending civil liberties, and will resist moves to trade one off against the other or to portray these objectives as mutually exclusive.

7. Going forward, the Government will take account of the responses to the Call for Evidence to inform its contribution to the forthcoming negotiations, and may seek additional evidence from stakeholders. The large volume of high quality responses to the Call for Evidence has provided a very helpful reflection of the range of interests and ideas in this area and the Government is grateful to all those who responded.

## **Consultation Co-ordinator contact details**

If you have any comments about the way this consultation was conducted you should contact the Ministry of Justice Consultation Co-ordinator at [consultation@justice.gsi.gov.uk](mailto:consultation@justice.gsi.gov.uk).

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

**Consultation Co-ordinator  
Legal Policy Team, Legal Directorate  
6.37, 6<sup>th</sup> Floor  
102 Petty France  
London SW1H 9AJ**

## 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 impact** – 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 exercises** – 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 questions asked in the Call for Evidence on the Current Data Protection Legislative Framework**

### **General**

**Q1: What are your views on the Data Protection Act 1998 and the European Directive upon which it is based? Do you think they provide sufficient protection in the processing of personal data? Do you have evidence to support your views?**

### **A. Definitions**

**Q2: What are your views of the definition of “personal data”, as set out in the Directive and the DPA?**

**Q3: What evidence can you provide to suggest that this definition should be broader or narrower?**

**Q4: What are your experiences in determining whether particular information falls within this definition?**

**Q5: What evidence can you provide about whether biometric personal data should be included within the definition of “sensitive personal data”?**

**Q6: If as a data controller you process biometric data, do you process it in line with Schedule 3 of the DPA which imposes an additional set of conditions?**

**Q7: Are there any other types of personal data that should be included? If so, please provide your reasons why they should be classed as “sensitive personal data”?**

**Q8: Do you have any evidence to suggest that the definitions of “data controller” and “data processor” as set out in the DPA and the Directive have led to confusion or misunderstandings over responsibilities?**

**Q9: Do you have any evidence to suggest that the separation of roles has assisted in establishing responsibilities amongst parties handling personal data?**

**Q10: Is there evidence that an alternative approach to these roles and responsibilities would be beneficial?**

**Q11: Do you have evidence that demonstrates that these definitions are helpful?**

### **B. Data Subjects' Rights**

**Q12: Can you provide evidence to suggest that organisations are or are not complying with their subject access request obligations?**

**Q13: Do businesses have any evidence to suggest that this obligation is too burdensome?**

**Q14: Approximately how much does it cost your organisation to comply with these requests?**

**Q15: Have you experienced a particularly high number of vexatious or repetitive requests? If so, how have you dealt with this?**

**Q16: What evidence is there that technology has assisted in complying with subject access requests within the time limit?**

**Q17: Has this reduced the number of employees required and/or time taken to deal with this area of work?**

**Q18: Is there evidence to suggest that the practice of charging fees for subject access requests should be abolished?**

**Q19: Do you have evidence to suggest that the £10 fee should be raised or lowered? If so, at what level should this be set?**

**Q20: Do you have evidence to support the case for a “sliding scale” approach to subject access request fees?**

**Q21: Is there evidence to suggest that the rights set out in Part Two of the DPA are used extensively, or under-used?**

**Q22: Is there evidence to suggest that these rights need to be strengthened?**

### **C. Obligations of Data Controllers**

**Q23: Is there any evidence to support a requirement to notify all or some data breaches to data subjects?**

**Q24: What would the additional costs involved be?**

**Q25: Is there any evidence to suggest that data controllers are routinely notifying data subjects where there has been a breach of security?**

**Q26: Do you have evidence to suggest that other forms of processing should also be exempt from notification to the ICO?**

**Q27: Do these current exemptions to notification strike the right balance between reducing burdens and transparent processing?**

### **D. Powers and Penalties of the Information Commissioner**

**Q28: What evidence do you have to suggest the Information Commissioner’s powers are adequate to enable him to carry out his duties?**

**Q29: What, if any, further powers do you think the Information Commissioner should have to improve compliance?**

**Q30: Have you had any experience to suggest that the Information Commissioner could have used additional powers to deal with a particular case?**

### **E. The Principle-based Approach**

**Q31: Do you have evidence to suggest the current principle-based approach is the right one?**

**Q32: Do you have evidence to suggest that the consent condition is not adequate?**

**Q33: Should the definition of consent be limited to that in the EU Data Protection Directive i.e. freely given, specific and informed?**

**Q34: How do you, as a data controller, approach consent?**

**Q35: Do you have evidence to suggest that data subjects do or do not read fair processing notices?**

### **F. Exemptions under the DPA**

**Q36: Do you have evidence to suggest that the exemptions are fair and working adequately?**

**Q37: Do you have evidence to suggest that the exemptions are not sufficient and need to be amended or improved?**

### **G. International Transfers**

**Q38: What is your experience of using model contract clauses with third countries?**

**Q39: Do you have evidence to suggest that the current arrangements for transferring data internationally are effective or ineffective?**

## **Annex B - List of respondents**

Abbey Quilting Limited

Abell Morliss International Limited

Action against Medical Accidents

Acxiom and Hunton & Williams (acting as secretariat for a group of interested organisations)

Acxiom Limited

Advertising Association

Amberhawk Training Limited

Associated Newspapers Limited

Association of British Insurers

Association of British Investigators

Association of Chief Police Officers

Association of Chief Police Officers Criminal Records Office

Association of Chief Police Officers in Scotland

Association of Medical Research Charities

Audit Scotland (also given on behalf of the Auditor General for Scotland and the Accounts Commission for Scotland)

Avon Information Management and Technology Consortium

AXA UK

Barclays

BBC

Bircham Dyson Bell LLP

Birmingham City Council

Bluefin Insurance Services Limited

Brewin Dolphin (Investment Managers)

Bristows

British Association for Adoption and Fostering

British Bankers Association (Joint response with the Association for Financial Markets in Europe)

British Insurers Brokers Association

British Retail Consortium

Brodies LLP

BSI Biometric Committee IST44

BSkyB

Callcredit

Campaign for Freedom of Information

Cancer Research UK

Centrica (British Gas)

Chaddesley Corbett Parish Council

Chartered Institute of Loss Adjusters

Children's Charities' Coalition on Internet Safety

CIFAS

Citizens Advice

City of York Council

Civil Court Users Association

Clear Skies Software

Commercial Workers Union

Confederation of British Industry

Consumer Focus

Data Protection and the Open Society

Department for Culture Media and Sport

Department for Environment Food and Rural Affairs

Direct Marketing Association

Driver and Vehicle Licensing Agency

Eduserv

Employment Lawyers Association

Energy Retail Association

Enfield Borough Police

Equifax Limited

Ernst & Young LLP

Everything Everywhere

Experian

Finance & Leasing Association

General Medical Council

General Social Care Council

GeneWatch UK

Hammonds LLP

Hampshire County Council

HeLEX Centre for Health, Law and Emerging Technologies, University of Oxford

Home Office

HSBC

Information Commissioner's Office

Intellect UK

International Financial Data Services

Internet Advertising Bureau

JANET (UK)

Keoghs LLP

Leeds City Council

Lewis Silkin LLP

Licensing Executives Society (Britain & Ireland)

Linklaters

London Metropolitan University

Market Research Society

Medical Research Council/Research Councils UK

Metropolitan Police Authority

Microsoft

Ministry of Justice

National Association of Data Protection Officers

National Grid PLC

National Information Governance Board for Health and Social Care

National Union of Teachers

NHS Information Centre

NHS National Services Scotland

NHS Wales Informatics Service

Norfolk County Council

Northumbria University

North Yorkshire County Council

Office of the First Minister and Deputy First Minister

Open Rights Group

Pearson

Periodical Publishers Association

Residential Landlords Association

Royal College of Physicians

Royal College of Physicians of Edinburgh

Royal Mail Group

Royal Society for the Protection of Birds

Simply DP Limited

Society of Editors

South East Post Adoption Network

Symantec

TechAmerica Europe

Tesco

Thames Water Utilities Limited

T H March & Co Limited

The Crown Prosecution Service

The Faculty of Advocates

The Foundation for Genomics and Population Health (PHG Foundation)

The Institute of Insurance Brokers

The Law Society of England & Wales

The Law Society of Northern Ireland

The Media Lawyers Association

The Metropolitan Police Service

The Mobile Broadband Group

The National Archives

The Newspaper Society

The Royal Academy of Engineering

The Royal Bank of Scotland

The Scottish Government

The Trades Union Congress

UK Border Agency

UK Council of Caldicott Guardians

UK Statistics Authority

Unilink Software Limited

University of Leeds

Vacuum Systems Limited

Verizon Business

Vodafone

Warner Bros

Wellcome Trust

Welsh Assembly Government

Western Health and Social Care Trust

Western Sussex Hospitals NHS Trust

West Yorkshire Police

Which?

World-Check

Yahoo

There were also twenty responses received from members of the public.



© Crown copyright  
Produced by the Ministry of Justice

Alternative format versions of this report are available on request from  
[informationrights@justice.gsi.gov.uk](mailto:informationrights@justice.gsi.gov.uk).