Ministry of JUSTICE

Annex A

Call for Evidence on the Current Data Protection Legislative Framework

List of questions for response

We would welcome responses to the following questions set out in this consultation paper. Please email your completed form to: informationrights@justice.gsi.gov.uk or fax to: 020 3334 2245. Thank you.

General

Question 1. **What are your views on the current Data Protection Act 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?**
Comments: It is clear that data subjects are being protected from data controllers but it is not at all clear what sort of harm a data controller might cause. Unfairness? Invasion of privacy? A clearer link to human rights, or a general right of privacy, would provide a background against which to assess success in fulfilling the principles. Nor is there any distinction between data controllers with more or less capacity for harm – eg having financial or organisational power, or perhaps being public authorities wielding the power of the state; nor is there anything about the relative vulnerability of data subjects – perhaps special protection is due to children or vulnerable adults. If children were identified as a special class of data subject, their parents' rights in relation to them should also be made clear. It is a complex area so perhaps a separate code would be necessary. There could be special protection owed to a child by a public authority.

Definitions

Question 2. **What are your views of the definition of "personal data", as set out in the Directive and the DPA?**
Comments: 1 "Relates to" is too vague. The Durant vs FSA judgement of the Court of appeal refers to

the subject being the focus of the information, it affecting his [or her] individual privacy, and it being biographically significant. This is a very useful and helpful approach and could be developed in a new Act or in guidance.

A data subject can be identified from the data relating to him or her – by whom? The definition does not clearly say by the data controller, so it could be by anyone. But a data controller does not know what everyone else might know, that would cause an item of data to identify a person. A data controller is at risk of finding that all data is personal, and must then manage that risk as best it can.

2 On the other hand the explanation of a relevant filing system in the same judgement is not at all helpful. The comparison made to a computer system's ease of access is too optimistic about how easily digital records can be searched. Consider looking for a digital photo without special face recognition software, or consider searching for references to a person in emails, where he is referred to only as "you-know-who", or his initials, or nick-names, or a very common name such as John or Smith. It is very difficult to design computer systems well; badly designed ones are very difficult to search. One possibility is for unstructured data, both paper and electronic, to be excluded or treated differently. There must be a more realistic view about how a large and diverse organisation can locate data in both paper and digital formats, with suitable criteria of ease and reliability.

The central problem here is how to balance practicality and cost with an obligation to each data subject that cannot be escaped by exploiting concepts such as "unstructured" or "informal". The definition as it stands makes it possible for a data controller to escape its obligations by deliberately bad record-keeping.

3 "The one child in the school" – the supposed identifiability of individuals from statistical information from very small populations leads to the possibility that anonymous facts might amount to personal data – especially if combined with other data held by (say) a newspaper. This vagueness and risk leads to excessive caution, and even cost; the ambiguity should be removed, one way or the other.

4 those who have died: In order to deal with the sudden loss of protection upon death, and the resulting probability of distress to relatives, we apply a "continuing duty of confidence" to the deceased. This amounts to doing with the data what we would have done if the Act did still apply. The definition should simply extend after death, either for a fixed period or until distress is not a problem. There could be a public interest exception for special cases.

5 What is an item of data? Perhaps a whole document, if someone is its focus. But another name, appearing only in the circulation list, may be evidence that that person attended a meeting or had an interest, which is a datum relating to that person and, if given focus in a new investigation, would amount to personal data. The use to which each word, and each clause, and each sentence, and each paragraph is being put, is relevant. “Data” is already plural but its size should be clarified to avoid doubt for both controllers and subjects.

6 The purpose or intention of the data controller – ie that a person should be a data subject – might be a useful test, as it is a well-used legal concept. It may be difficult to prove intention, but a reputable data controller (especially a public authority) could direct its resources to where protection would be most beneficial and stop worrying about incidental or trivial references.

Question 3. **What evidence can you provide to suggest that this definition should be made broader or narrower?**

Comments: We have not done any systematic research into this problem but see below for anecdotal evidence.

Question 4. **What are your experiences in determining whether particular information falls within this definition?**

Comments: It is a common experience in DP subject access requests that many trivial references to the data subject are found (eg name mentioned in an email about arranging a meeting of completely different people) that must then be considered using the tests above. The same applies in FoI requests where data should be refused because it may be personal data.

Considering focus and current purpose is a very time-consuming activity.

Parents usually act as if they had an automatic right over their children and using age 12 as a general marker of capability can lead so confusion. For instance in an education context correspondence is usually between the school and parent, and if the parents subsequently request to see their child’s education file it seems to them anomalous to then require consent from the child

Question 5. **What evidence can you provide about whether biometric personal data should be included within the definition of "sensitive personal data"?**
Comments: Biometric data is just an identifier, like a name or NI number, unless sensitive data is somehow encoded in it, such that it can be retrieved and used. If such encoding is present, then it already amounts to sensitive data and Schedule 3 applies; if not, it does not.

Question 6. **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?**
Comments: n/a

Question 7. **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"?**
Comments: Bank account or credit card numbers, on the grounds that loss or compromise is likely to permit a fraud. However this is a very different concept of sensitivity to that at Q 5. It relates to the seventh principle (security) rather than to special conditions under the first principle. Nevertheless the concept of sensitive data, and how it is applied, could be redefined to take account of risks to individuals by others, rather than to large groups of individuals by the state.

Question 8. **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?**
Comments: Where the relationship is client to contractor the definition is easy. Where the relationship is a partnership they may wish to be "data controllers in common" – a useful concept that could be defined in a new Act.

Question 9. **Do you have any evidence to suggest that the separation of roles has assisted in establishing responsibilities amongst parties handling personal data?**
Comments: Examples are data sharing agreements with other public sector partner bodies (separate controllers); joint service provision (eg Aim Higher or ContactPoint, where

partners are or were controllers in common); contracts for customer satisfaction surveys where a contractor is a data processor. A processor has no interest in the data, except for carrying out the contract.

The conditions at Sch 1 para 12 could include the fifth principle – the processor does not retain the personal data after completion of the contract.

Question 10. **Is there evidence that an alternative approach to these roles and responsibilities would be beneficial?**

Comments: No

Question 11. **Do you have evidence that demonstrates that these definitions are helpful?**

Comments: See Q9.

Data Subjects' Rights

Question 12. **Can you provide evidence to suggest that organisations are or are not complying with their subject access request obligations?**

Comments: The Council tries to fulfil its obligations but it is difficult and time-consuming to locate all the data that may be disclosable and then make the decisions. Therefore it sometimes exceeds the 40 days, and may inadvertently fail to disclose. This is not malicious or careless refusal to comply, but rather the practical problem of finding everything that must be disclosed and knowing it's all been found; having recording systems that are designed to deliver services, rather than dedicated to data subjects' rights (and so not always arranged by reference to every possible data subject to be found there), and the time needed to consult other parties whose rights may be affected (both staff and other members of the public, and especially within families).

Question 13. **Do businesses have any evidence to suggest that this obligation is too burdensome?**

Comments: No evidence but please see responses to Q. 12 and Q.14.

Question 14. **Approximately how much does it cost your organisation to comply with these requests?**
Comments: It is not possible to quantify the total cost of complying with such requests but it is considerable in terms of locating and retrieving the information, reviewing it to consider whether it is a) personal data b) subject to any exemption, contacting any necessary third parties. Time and costs are increasing year by year

Question 15. **Have you experienced a particularly high number of vexatious or repetitive requests? If so, how have you dealt with this?**
Comments: No.

Question 16. **What evidence is there that technology has assisted in complying with subject access requests within the time limit?**
Comments: On the contrary, technology creates more data in more places that must be manually searched for what is, or is not, relevant or personal.

Question 17. **Has this reduced the number of employees required and/or time taken to deal with this area of work?**
Comments: No.

Question 18. **Is there evidence to suggest that the practice of charging fees for subject access requests should be abolished?**
Comments: £10 is too small to be worth collecting and for the majority of requests does not nearly cover the cost to the Council of processing a request.

Question 19. **Do you have evidence that the £10 fee should be raised or lowered? If so, at what level should this be set?**
Comments: The reasoning that led to setting the £10 limit can be re-applied to present-day costs. Suggest £50.

Question 20. **Do you have evidence to support the case for a "sliding scale" approach to subject access request fees?**
Comments: There is a huge variation in the volumes of data relevant to different requests – both data to be considered and data to be disclosed. A sliding scale would permit large-volume enquiries to be negotiated down to a level acceptable to data controller and data subject.

Question 21. **Is there evidence to suggest that the rights set out in Part Two of the DPA are used extensively, or under-used?**
Comments: These rights are not used very often, probably because disputes and complaints are settled using service-delivery solutions (and language) rather than data processing solutions and language.

Question 22. **Is there evidence to suggest that these rights need to be strengthened?**
Comments: n/a.

Obligations of data controllers

Question 23. **Is there any evidence to support a requirement to notify all or some data breaches to data subjects?**
Comments: It is hard to see how this would be expressed in a directive or an Act; Information Commissioner guidance is more appropriate, and is very good.

Question 24. **What would the additional costs involved be?**
Comments: Researching the breach; identifying the affected subjects; making contact; managing the publicity. Greater likelihood of have to defend, or even pay, a compensation claim. The Council already does the first two (research and identify affected subjects) and takes a case by case view on information the affected subjects. Organisations would require further guidance on what constitutes a security breach if this was to be a legislative requirement. What about a lost file (where no-one knows what has happened to it) or a letter sent to the wrong address and seemingly not opened etc. Would the data subject have the right to know

the identity of the person to whom the data has been disclosed (which they will be very likely to want to know.)

Question 25. **Is there any evidence to suggest that data controllers are routinely notifying data subjects where there has been a breach of security?**
Comments: In particular circumstances the council does so.

Question 26. **Do you have evidence to suggest that other forms of processing should also be exempt from notification to the ICO?**
Comments: No.

Question 27. **Do these current exemptions to notification strike the right balance between reducing burdens and transparent processing?**
Comments: n/a

Powers and penalties of the Information Commissioner

Question 28. **What evidence do you have to suggest the Information Commissioner's powers are adequate to enable him to carry out his duties?**
Comments: He now has powers to fine which have not been fully tested. No additional powers needed until the new power to fine has been evaluated.

Question 29. **What, if any, further powers do you think the Information Commissioner should have to improve compliance?**
Comments: Consider a stronger right to audit or assess processing

Question 30. **Have you had any experience to suggest that the Information Commissioner could have used additional powers to deal with a particular case?**
Comments: No

The Principles-based Approach

Question 31. **Do you have evidence to suggest the current principles-based approach is the right one?**
Comments: It is an "output-based" approach that allows the huge range of data-controlling organisations each to arrange its own affairs, and be judged on the results. An explicit approach would be hard to make suitable for all data controllers, from a small school to a large county council, or from a corner shop to an international bank

Question 32. **Do you have evidence to suggest that the consent condition is not adequate?**
Comments: No evidence

Question 33. **Should the definition of consent be limited to that in the EU Data Protection Directive i.e. freely given specific and informed?**
Comments: Yes

Question 34. **How do you, as a data controller, approach consent?**
Comments: We prefer to use another schedule condition wherever possible, and avoid relying on consent. Telling data subjects what's happening is not the same as asking consent. Telling them through a fair processing statement is essential, as they cannot possibly exercise their rights unless they know who is controlling their data.

Question 35. **Do you have evidence to suggest that data subjects do or do not read fair processing notices?**
Comments: No.

Exemptions under the DPA

Question 36. **Do you have evidence to suggest that the exemptions are fair and working adequately?**

Comments: A different rule for references written and those received does not make sense. The data subject can ask both writer and receiver as they are both data controllers but they have different duties. Suggest remove exemption? Data subjects use S7 when there is (or might be) a dispute, to discover evidence. This risks putting the data controller's preparation of the case at risk. An exemption would allow disclosure of all evidence to take place under the usual procedure.

Question 37. **Do you have evidence to suggest that the exemptions are not sufficient and need to be amended or improved?**
Comments: Section 35 relies only on a test of necessity. A better test would be public interest or proportionality, to balance the benefit to the person disclosed to against the harm to the data subject. This could also apply to Section 29. But as this would be still be a largely subjective decision thorough guidance should be provided.

International Transfers

Question 38. **What is your experience of using model contract clauses with third countries?**
Comments: None.

Question 39. **Do you have evidence to suggest that the current arrangements for transferring data internationally are effective or ineffective?**
Comments: No.

About you

Please use this section to tell us about yourself

Full name	Robert Beane
Job title or capacity in which you are responding to this consultation exercise (e.g. member of the public etc.)	Information Management Officer
Date	
Company name/organisation (if applicable):	City of York Council
Address	PO Box 31, Library Square
	York
Postcode	YO1 7DU
If you would like us to acknowledge receipt of your response, please tick this box	☐ (please tick box)
Address to which the acknowledgement should be sent, if different from above	

If you are a representative of a group, please tell us the name of the group and give a summary of the people or organisations that you represent.