



Data Sharing Review Secretariat  
5.26 Steel House  
11 Tothill Street  
London  
SW1H 9LH

By post and e-mail: [contact@datasharingreview.gsi.gov.uk](mailto:contact@datasharingreview.gsi.gov.uk)

14 February 2008

**USE AND SHARING OF PERSONAL INFORMATION IN THE PUBLIC AND PRIVATE SECTORS - SOCIETY FOR COMPUTERS AND LAW PRIVACY AND DATA PROTECTION INTEREST GROUP RESPONSE TO THE DATA SHARING REVIEW CONSULTATION PAPER DATED 12 DECEMBER 2007**

**1 INTRODUCTION**

The Society for Computers and Law ([www.scl.org](http://www.scl.org)) welcomes this opportunity to respond to the Data Sharing Review Secretariat (the “**Secretariat**”) consultation (the “**Consultation**”) on the use and sharing of personal information in the public and private sectors.

However, we were a little disappointed that the Consultation appears to come before any review – we would have thought a survey of key experts and practitioners could have been undertaken by the Secretariat so that the Consultation could have been on its findings of the way the Data Protection Act 1998 (“**DPA**”) operates and its proposal for options for implementing any changes.

We suspect that we are not alone among organisations in considering that the scope and open-ended nature of the Consultation inhibited participation and comment.

**2 CONSULTATION LIST OF QUESTIONS FOR RESPONSE**

Our responses to questions set out in the Consultation are set out in the Annex to this response. We have restricted ourselves to responding to Section 1, to provide background on the interests of SCL and its Privacy and Data Protection Interest Group in this area, and to our commentary on the law under the relevant questions at Section 3.

**3 CONCLUSION**

In conclusion, our recommendations are that:

- 3.1 the Information Commissioner be given enforcement powers that are much more rigorous - we believe that the ability to impose administrative fines of up to 10% of turnover of data controllers ought to be considered;

- 3.2 if the Information Commissioner continues not to have the resources to enforce the DPA effectively, that alternative enforcement mechanisms be considered – we believe that a mandatory data protection audit obligation may be an effective mechanism in this regard; and
- 3.3 the Information Commissioner should be given the power to issue binding rules on data protection, in a similar fashion to, for example, to those powers granted to the Financial Services Authority under the Financial Services and Markets Act 2000.

**Society for Computers and Law (Privacy and Data Protection Interest Group)  
14 February 2008**

**NOTE:-**

The Society was created in 1973 to encourage and develop IT for lawyers and IT related law. The Society is “*Where Computers and Law meet*”, and provides a forum for members to meet and exchange information and ideas or raise issues of concern with others. Through its membership, its widely acclaimed magazine *Computers & Law*, regional meetings and national conferences, the Society promotes issues of importance in the field of IT Law and the implementation of IT within legal and related practices.

**CONTACTS:-**

For further information about the Society’s views on the Consultation or other data protection related issues, please contact:

**David Berry**, Partner, Charles Russell LLP, SCL Privacy and Data Protection Interest Group, Chairman (email: david.berry@charlesrussell.co.uk; tel: 020 7203 5170), or in his absence, **Andrew Sharpe**, Partner, Charles Russell LLP (email: andrew.sharpe@charlesrussell.co.uk; tel: 020 7203 5194).

For further information about the Society, please contact:

**Ruth Baker**, General Manager, Society for Computers and Law, 10 Hurle Crescent, Bristol BS8 2TA (email: ruth.baker@scl.org; tel:: 0117 9237393; fax: 0117 9237393)

## Annex to SCL Response

### Use and sharing of personal information in the public and private sectors

#### Section 1:Background

Question 1. Please explain what your interest in information sharing is.

Answer/Comments:

The Society for Computers and Law is the leading organisation in the UK concerned with the law relating to the practice and development of IT with more than 1,500 members from the IT industry and in legal practice. The Privacy and Data Protection Interest Group has a specific remit to monitor developments in data protection and security, data sharing, freedom of information and other privacy issues with an IT interface.

On 7 November 2007 the Group arranged a seminar at DLA Piper UK LLP on data sharing that was well attended by many of the UK's leading privacy authorities. Talks were given by Usha Jagessar of DLA Piper UK LLP, Iain Bourne of the Information Commissioner's Office and Helen Child, formerly of Transport for London.

The Group has an active interest in data sharing policy, and has followed the Data Sharing Review Consultation with interest.

### **Section 3: The legal framework**

Question 9. In your view, how well does the DPA work? Please outline the DPA's main strengths and weaknesses and any proposals for changes you would like to see made, including suggestions for their implementation.

Answer/Comments:

We consider that the DPA has been moderately successful, but is in need of review and debate to judge how effective it is in protecting the public against the "real" data protection threats they face in 2008. It is much more effective than the legislation it replaced and it has done much to raise public awareness of data security. However, we note that there continue to be problems of understanding the purposive, framework approach taken by the DPA.

As legal practitioners we are used to dealing with a steady stream of queries concerning the application of the DPA to ordinary business activities and handling requesting guidance. The fact the DPA is only intended to provide a framework in terms of the Data Protection Principles which data controllers are required to apply is not appreciated by many data controllers. Businesses appear not to understand what is being required of them by the DPA; they would prefer more prescriptive laws and regulations to give them more certainty as to their DPA obligations.

As an example, one view of the Seventh Principle is that it gives a clear obligation that is technologically and procedurally neutral. Together with the guidance on what is meant by the Seventh Principle in paragraphs 9 to 12 of Schedule 1 to the DPA, it should be a straightforward Principle to apply. However, many data controllers appear uncomfortable with the fact that the Principle requires them to assess for themselves the question of appropriateness. Even after nearly ten years of the DPA, data controllers have not got used to the lack of prescriptive regulations on matters such as organisational and technical security measures, with a result that many, as has recently been shown by many high profile cases of accidental loss, do not have appropriate technical or organisational security measures in place.

The main benefits of the DPA have been:

1. Raising public awareness of personal data and data security issues.
2. Creating a comprehensive and reasonably flexible structure for the assessment and handling of personal information by data controllers and processors. The principles are sufficiently wide-ranging to cover most areas of public concern.
3. Instituting an administrative structure that deals with complaints and acts both as an impartial referee (the Information Commissioner has been notably successful in setting himself and his department at a distance from government), and an effective promoter of

Question 9. In your view, how well does the DPA work? Please outline the DPA's main strengths and weaknesses and any proposals for changes you would like to see made, including suggestions for their implementation.

good practice in personal data processing. The Information Commissioner's Office (the ICO) deals with more than 23,000 complaints a year and the figure is rising. It does so efficiently, and with a comparatively limited budget.

The main drawbacks of the DPA are:

1. Lack of any delegated powers to the Information Commissioner to make binding rules to clarify the general requirements of the Data Protection Principles (cf. the Financial Services Authority and the status of the FSA Handbook under section 138 of the Financial Services and Markets Act 2000), or the lack of funding mechanisms to ensure the Information Commissioner's Office is adequately resourced for developing any such rules and associated guidance and their enforcement.
2. Lack of effective sanctions. Many institutions do not have the "fear" to comply. In the private sector there is at least the risk of reputational damage to act as a driver for compliance. In the public sector, there is arguably no similar incentive. Data security issues are often discussed and adverted to personnel in many organisations; they are often routinely ignored. The Information Commissioner's suggestion of criminal penalties and widening the scope of assessment and enforcement might "raise the bar" of compliance. We note, as has the Information Commissioner, that the enforcement powers of the Commissioner and the lack of any power to impose administrative fines are in stark contrast to those of bodies such as the Financial Services Authority and the Office of Fair Trading.
3. The lack of a clear definition of what is "personal data". The legacy of *Durant –v- Financial Services Authority*, and the relatively narrow interpretation of the DPA by the courts, has not only exposed the UK to attack by the European Commission, but has increased uncertainty as to what is within the scope of the DPA. We note with approval the proposals of the Article 29 Data Protection Working Party to clarify the definition of "personal data" to include "information available in any form", "objective information" and "biometric data", and the emphasis placed on the "content", the "purpose" and the "result".
4. Some of the nomenclature used in the DPA, such as "relevant filing system", "data controller" and "data processor", cause confusion because of their wide-ranging application. The separate treatment of data and "sensitive personal data" may also sow confusion, particularly as personal financial data is not included in the definition of

Question 9. In your view, how well does the DPA work? Please outline the DPA's main strengths and weaknesses and any proposals for changes you would like to see made, including suggestions for their implementation.

"sensitive personal data" even though this is often personal information that data subjects consider to be the most sensitive other than data concerning physical or mental health or condition. We believe that instead of having a predefined class of "sensitive personal data", data controllers should be required to carry out risk assessments on their processing of personal information, so that any processing, either because of its scope or the nature of the personal information being processed, that would or would be likely to cause the data subject unwarranted, substantial damage or distress (using the form of words at section 10, or such other measure) if there were a breach of the data protection principles in respect of that processing, would be subject to the greater restrictions. Such a risk-based regime could also remove the current distinction between personal information in a "relevant filing system", which is subject to the DPA, and information which is not.

5. Whilst subject access rights in section 7 are adequate, the enforcement provisions are not (section 7 (9)), and the recourse to court would deter most subjects. The same problems arise in relation to sections 13 and 14: the emphasis on litigation, rather than to the ICO or Information Tribunal, deters most subjects from enforcing their rights directly. Whilst the ICO does actively pursue data controllers who deny data subjects their rights, there needs to be more of a deterrent against any denial of rights.
6. There ought to be separate sanctions in respect of breaches of data subject's direct marketing rights (section 11). The DPA has had only a moderate effect in reducing quantities of spam and marketing materials. We believe that there needs to be a reform of direct marketing law, particularly as the Privacy and Electronic Communications (EC Directive) Regulations 2003 sit outside of the DPA.
7. The powers of the ICO to enforce proper data management and the collection of information under sections 40, 43, 44, 46 and 47 appear to be protracted and could have the effect of impairing the efficiency of the ICO. These provisions may have been suitable when the DPA was in gestation, but they seem too rigid and cumbersome in the context of the strong growth in the number of complaints handled by the ICO. These powers could be strengthened in accordance with the Information Commissioners' suggestions. In particular:
  - The ability to impose spot fines and to create greater search powers than those detailed in section 50 and Schedule 9 could be considered.

Question 9. In your view, how well does the DPA work? Please outline the DPA's main strengths and weaknesses and any proposals for changes you would like to see made, including suggestions for their implementation.

- In section 51 (4) the ICO should have the right to impose codes of conduct on public sector bodies as well as trade associations.
- Consent by controllers to inspections by the ICO should not be required.

8. The notification regime at Part III of the DPA does not serve any practical purpose, other than the mechanism by which the ICO collects approximately £10m per year in fees. As the £35 annual registration fee is almost a universal tax, it would be more efficient if the ICO's data protection work were funded by a grant in aid. We suspect that any such grant in aid would be more than offset by the amount of administrative fines that would be paid into the Consolidated Fund, if the ICO were to give enforcement powers to levy fines similar to, for example, the OFT or FSA.

Question 10. In your view, how well do public authorities and private organisations adhere to the Second Principle of the DPA? How valuable do you believe the Second Principle is? Please provide examples and reasoning behind your response.

Answer/Comments:

Our anecdotal experience of compliance with the Second Principle is that the private sector is poor at giving proper fair processing notices to data subjects, but that there is little "second use" of personal data once it has been obtained from data subjects or third parties other than the commercialisation of customer lists. The sharing of information for marketing purposes appears to be the major problem area, which involves breaches of the Second Principle, abuse of the data subjects' rights under section 11 and breaches of the Privacy and Electronic Communications (EC Directive) Regulations 2003.

With the public sector the obligation to have Freedom of Information publication schemes appears to have ensured that most public authorities publish full fair processing notices together with such schemes. However, there is growing pressure on public authorities to share information as part of initiatives such as Transformational Government. We therefore consider that the Second Principle is an important safeguard against function creep, but it is only effective to the extent that the original purpose or purposes are fairly given by the relevant public authorities. The question of the quality of consent also becomes an issue in this context, as clearly citizens have no effective choice but to submit their personal data to public sector organisations in order to receive state services or to comply with their legal obligations.

Question 10. In your view, how well do public authorities and private organisations adhere to the Second Principle of the DPA? How valuable do you believe the Second Principle is? Please provide examples and reasoning behind your response.

We therefore believe that the Second Principle is only effective to the extent that the First Principle is also complied with. For this reason, we consider that a single “fair and lawful” principle would be more appropriate. It should be clear that the processing of personal information outside of a specified and lawful purpose is unfair and unlawful. Data controllers should be under clear obligations to make readily available to data subjects these specified and lawful purposes - to this end data controller should be required to publish their registrable particulars (as defined at section 16(1)).

Question 11. What technical, institutional or societal barriers stand in the way of the effectiveness of the DPA? Please provide examples.

Answer/Comments:

The main impediments are:

1. Ignorance and misunderstanding of the DPA and the work of the ICO. Data protection is an issue that seems to provoke indifference and indignation: long periods of indifference punctuated by spasms of indignation.
2. The belief that the “cure is worse than the illness”, and that government regulation of personal information is a burden to business and a fetter on the free movement of goods, capital – and information.
3. The occasional tendency for a response to regulation to have an unintended consequence, usually as a result of a misunderstanding of the DPA – well known examples including the failure by British Gas to notify Social Services of their cutting of pensioners’ gas supply and the inappropriate data retention policies adopted by Humberside Constabulary pre Soham and post the Bichard Report. The DPA tends to encourage a process-driven approach to data management, which creates its own abuses. Data retention is often poorly managed – this is a resource issue in many organisations.
4. The lack of prescriptive regulations or detailed guidance (although we note that more recently there has been more guidance forthcoming from the ICO) – as noted above, the purposive approach taken by the DPA appears to cause data controllers problems, as particularly under the English system data controllers appear to want more narrowly defined obligations.

Question 12. What further powers, safeguards, sanctions or provisions do you believe should be included in the DPA?

Answer/Comments:

The Information Commissioner has argued persuasively in favour of increased powers and enforcement rights. We endorse the view that the ICO ought to have the ability to impose administrative fines to the level of 10% of turnover of data controllers, with the right to audit any data controller without notice.

We agree that “knowingly and recklessly” handling data should be made an offence. We note with approval the suggestions of a new offence of “information abuse”. This might make individuals more circumspect about leaving laptops in public places. We believe that a more aggressive and subject-friendly approach be taken towards enforcement and the imposition of penalties: spot fines on a sliding scale; a national “register of shame”; public apologies full page advertisements in national newspapers; the imposition of an onerous, due diligence regime on miscreants under the ICO’s supervision, etc. could all be considered.

We agree that the ICO should not need to obtain the consent of controllers/processors before making inspections. There is no reason why it should not be able to conduct “dawn raids” in a manner similar to the competition authorities, for example.

If the ICO is to continue to be funded by the present model, i.e. inadequately, then we believe that consideration ought to be given to requiring certain data controllers to be required to submit themselves to independent data protection audit, with a submission of the auditor’s report to the ICO. The data controllers who should be subject to this requirement could either be of a certain size in terms of numbers of data subjects’ records or those who are not eligible to be exempt notification under the Data Protection (Notification and Notification Fees) Regulations 2000. There is an argument that public sector organisations to whom data subjects are compelled either by law or practice to submit personal information should be required to publish such audit reports, notwithstanding that they may be disclosable pursuant to a request for information under the Freedom of Information Act 2000.

Whilst we recognise that an audit requirement may be an expensive exercise for some organisations, we note that for well-organised and DPA-compliant data controllers the process of submitting to an audit in the same or similar structure to the Data Protection Audit Manual published by the Information Commissioner should not be a significant regulatory burden. Such data controllers would easily “pass” an Adequacy Audit, and would not be subject to a lengthy or expensive Compliance Audit.

Question 13. Are there any other aspects of UK or EU law (such as EU Directive 95/46/EC) that impact positively or negatively on data sharing or data protection? Please provide examples.

Answer/Comments:

Whilst we note that the House of Lords may give a definitive ruling on what is “personal data” for the purposes of the DPA in *Common Services Agency –v- Scottish Information Commissioner*, we consider that the uncertainty over whether the definition of “personal data” under *Durant –v- Financial Services Authority* is compliant with the EU Directive 95/46/EC is unhelpful.

In the context of data sharing in the public sector, we are concerned that the inclusion of a wide data sharing purpose in public sector fair processing notices, such as, for example, “our sharing of your personal information with other [government departments][public authorities] in order to increase the efficiency and effectiveness of our or their provision of services to you”, together with lawful processing purpose at, for example, paragraph 6(1) of Schedule 2 to the DPA (Article 7(f) of the EU Directive 95/46/EC), may not be fair processing even though it appears lawful. This is because the citizen has no effective choice in supplying or permitting many government departments or public authorities from processing their personal information. We consider that any data sharing regime should consider requiring unambiguous consent for sharing or processing that is beyond the direct and necessary purposes of the relevant data controller.

Question 14. Are there any statutory powers unavailable that would enable better and more secure sharing of personal information – for example for identity authentication purposes – between a) public authorities and b) public authorities and private organisations? If so, what are they? Please provide examples and any steps you believe could be taken to improve matters.

Answer/Comments: We have no comment to make on this question.

Question 15. Are there any parts of the legal framework that place an unreasonable burden on business? Please provide examples.

Answer/Comments:

We have commented upon the notification regime at Part III of the DPA above. We do not believe that the DPA places unreasonable burdens on business, but we do believe that a risk-based approach to the application of the DPA should be encouraged.