

**BASINGSTOKE & DEANE BOROUGH COUNCIL**

**RESPONSE TO CONSULTATION PAPER ON THE USE AND SHARING OF  
PERSONAL INFORMATION IN THE PUBLIC AND PRIVATE SECTORS**

**Replies to Questionnaire**

**Section 1: Background**

**QUESTION 1**

Please explain what your interest in information sharing is.

If you have an active involvement in personal information sharing, we would be grateful for the following information:

- What kinds of personal information do you collect, hold and share?
- How do you collect, hold and share such personal information:
- For what purposes do you collect, hold and share such personal information?

**Reply:**

Using the work of the Council's Fraud Investigation Team as an example, there are many instances where it is necessary to share information in order to gain and collate the necessary evidence in the course of the investigation. This process is often extremely difficult, time consuming and delayed by those people who have little or no understanding of Data Protection issues.

The team collects, holds and shares a vast amount of personal information:

Names  
DOB  
NI Numbers  
Addresses  
Dependants  
Non-dependants  
Place of employment  
Earnings  
Savings accounts with account numbers  
Bank accounts with account numbers  
Any other capital in any form  
Proof of residence such as utility bills  
Proof of identify such as passport

Information is collected through the course of the investigation. A lot of the information would come into the Authority on the initial claim. In addition through

the course of the investigation additional information may be requested from the claimant and also from any employer, HMRC and the DWP.

**Section 2: Scope of personal information sharing, including benefits, barriers and risks of data sharing and data protection**

**QUESTION 2**

What in your view are the key benefits of sharing personal information to:

- (a) individuals, and
- (b) society?

Please provide examples.

**Reply:**

The key benefit of sharing personal information to either individuals or societies is that the true picture can be established. In addition, this picture will not only be true, it will be complete and hopefully done quickly. Although there must be safeguards it should not be such a long winded job to prove someone has committed theft or other forms of deception.

Within the context of the work of the Fraud Investigation Team there is considerable Data Sharing between our Authority and other Local Authorities. For example, when a claimant moves from one Local Authority area to another we are able to obtain details of the person's previous applications for benefit.

**QUESTION 3:**

What in your view are the key risks of sharing personal information to:

- (a) individuals, and
- (b) society?

Please provide examples.

**Reply:**

The key risks in providing information are, in our view, ensuring that you and they have the authority to send and receive it, what is it going to be used for, and the controls in place to ensure it is not used for anything else, and the storage of that information.

Examples of this, for us, would be the data submitted by a third party as part of the National Fraud Initiative.

Investigation files are sometimes submitted to the DWP for an adjudication decision. As the DWP uses a centralised approach this often means sending the file in the post. This raises security issues for both parties.

**QUESTION 4:**

As mentioned in the introduction, there are wide variations in the scope and methods of personal information sharing. What scope and what methods, in your view, post the greatest opportunities or risks? Please explain the reasoning behind your response.

**Reply:**

The greatest risk in sharing personal information must be having to send information and files in the post with the risk that information is lost. This is primarily to the DWP as stated above.

**QUESTION 5:**

Please provide examples of where, in your view, the public authorities hold too much data or not enough personal information, and the reasoning behind your response.

**Reply:**

We consider that public authorities neither hold too much or too little information.

**QUESTION 6:**

Please provide examples of where, in your view, private sector organisations hold too much personal information or not enough personal information, and the reasoning behind your response.

**Reply:**

No comment.

**QUESTION 7:**

Please provide examples of cases where you believe the sharing of personal information between two or more bodies would be beneficial, but where it is not currently taking place.

Please explain as fully as possible why information is being shared, detailing what the barriers to the sharing of personal information are – eg legal, cultural, financial, institutional – and how these barriers can be overcome.

**Reply:**

The ability to access the car insurance database would be extremely useful. At the moment it is very hit and miss to how one obtains this information. The problem with all this is that we are all supposedly in the same game but everyone has different rules.

**QUESTION 8:**

Please provide examples of cases where you believe that personal information is being shared between two or more bodies, but where this should not be taking place.

Please describe the information-sharing concerned and why you believe it should not be taking place, including the risks involved in such information-sharing.

**Reply:**

No comment.

**Section 3: The legal framework**

The Data Protection Act (DPA) regulates the processing of information, including its obtaining, holding, use and disclosure.

The second principle of the DPA is as follows:

“Personal data shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes.”

**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.

**Reply:**

The DPA is good as it stands. However, the main problem is interpretation. More often than not you hear “I can't give you that under DPA”. When questioned further the person is unable to specify exactly what part of the DPA they are referring to. We suggest the use of information for fraud prevention should be much more widely communicated and the exchange of said information must be simplified. It might be a good idea to have clear guidelines on the use and dissemination of Personal Data under the Date Protection Act.

**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 the reasoning behind your response.

**Reply:**

Some authorities and departments adhere to the second principle to the eighth degree. Others will show some common sense. The problem across the board is one of consistency. This could be within public authorities or within the private sector.

**QUESTION 11:**

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

**Reply:**

The most common barrier we find is the institutional barrier. What we mean by this is that some organisations adopt an almost totally negative response to everything and hide behind the DPA. Others are more open in their willingness to disclose/share information. This area could be clarified by guidelines.

**QUESTION 12:**

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

**Reply:**

No comment.

**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.

**Reply:**

No comment.

**QUESTION 14:**

Are there any statutory powers unavailable that would enable better and more secure sharing of personal information – for example for identify 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.

**Reply:**

A suggestion would be a database of authorised personnel within organisations and authorities that would be available to all persons. Instead of having to jump through hoops to exchange information, each person on the database would have their own identification code which would be exchanged with the person holding the information. These codes could change randomly and be verified centrally a bit like chip and pin, etc.

**QUESTION 15:**

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

Please outline your proposals for streamlining the legislation to ensure that such burdens are minimised.

**Reply:**

No comment.

**Section 4: Consent and Transparency**

**QUESTION 16:**

Is it clear whether and when you need individual's consent to share information about them? Are you clear about the form that consent should take? Please provide examples.

Please provide details of any initiative you have been involved in that has been based on consent.

**Reply:**

No, it is not always clear to all parties. In some simple exercise such as dealing with an enquiry on behalf of someone you will often come up against the DPA. It needs to be much simpler to actually help people. People are put off in many instances because the DPA is often quoted.

**QUESTION 17:**

What, if any, barriers would a requirement for gaining consent create to the sharing of personal information? Please explain your reasoning.

**Reply:**

No comment.

**QUESTION 18:**

Do you have any suggestions on how to make the sharing of information more transparent?

For example, should individuals be given strengthened access rights? And, if so, how? Should organisations be expected to do more to explain their use of sharing of personal information to the public? And if so, how?

**Reply:**

We consider the reasons information could and should be used should be more widely known. Exactly how this can be done would be a matter for clearer legislation and guidance.

**QUESTION 19:**

How can we best ensure that information sharing policy is developed in a way that ensures proper transparency, scrutiny and accountability?

For example:

In your view, how valuable is the Information Commissioner's recently published Framework code of practice for sharing personal information

([http://www.ico.gov.uk/upload/documents/library/data\\_protection/detailed/specialist/guides/pinfo-framework.pdf](http://www.ico.gov.uk/upload/documents/library/data_protection/detailed/specialist/guides/pinfo-framework.pdf))?

In your view, how valuable are privacy impact assessments along the lines announced by the Information Commissioner on 11 December ([www.ico.gov.uk](http://www.ico.gov.uk))?

**Reply:**

No comment.

## **Section 5: Technology**

### **QUESTION 20:**

What impact, in your view, have technological advances had on the sharing and protection of personal information? Please provide examples.

#### **Reply:**

No comment.

### **QUESTION 21:**

Should the law mandate specify technical safeguards for protecting personal information?

For example, should there be an explicit requirement that all personal information held on portable devices be encrypted to a particular standard?

#### **Reply:**

No comment.

### **QUESTION 22:**

How, in your view, could 'privacy enhancing techniques', such as the anonymisation or pseudonymisation of personal information, help safeguard personal privacy, whilst facilitating activities such as performing medical research?

Is sufficient advice about the deployment of such techniques available? Are you confident about using them? What are the barriers to using them?

#### **Reply:**

Technology should be able to play its part in data sharing by the use of access passwords and confirmation passwords. See reply to Question 14.

## **Section 6: International comparisons**

### **QUESTION 23:**

Are you aware of any jurisdictions whose legal framework for sharing and protecting personal information contains features that could be useful in a UK context? Please provide examples.

### **QUESTION 24:**

Do you have any international examples of good practice in the sharing of personal information that could or should be adopted by the UK?

**QUESTION 25:**

Do you have any knowledge of jurisdictions that have adopted a particularly permissive or restrictive approach to sharing personal information? What have the consequences of this been?

**QUESTION 26:**

Are you aware of significant differences in public attitudes to the sharing of personal information in other countries? Please provide examples and an explanation for why you believe this to be the case.

**Reply: Questions 23-26**

No comment.

**Section 7: Additional questions**

**QUESTION 27:**

Are there any additional issues on the sharing of personal information and protection of personal information that this review should be considering?

Do any of these issues apply specifically to your sector?

**QUESTION 28:**

Please set out any additional suggestions or observations you have that you believe will be of assistance to the review.

**Reply: Questions 27 and 28**

It would be extremely beneficial to all parties that the use and exchange of information between organisations and authorities in the fight against crime could be made more open, transparent, quicker and less bureaucratic.