

Data Sharing Review

Richard Thomas and Dr Mark Walport

Consultation paper on the use and sharing of personal information in the public and private sector

List of questions for response

We would welcome responses to the following questions set out in this consultation paper. Please follow the question order as set out in the consultation paper, leaving a blank response box for any questions not answered.

Please email your completed form to contact@datasharingreview.gsi.gov.uk

Alternatively you can send a hard copy response to:

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

Thank you.

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?

Comments:

The Data Protection Forum is an association of organisations from all sectors, formed to provide a focus for the exchange, analysis and communication of information on all matters relating to the protection of personal information and compliance with Data Protection law, and more recently compliance with Freedom of Information.

The Forum gives members the opportunity to take part in discussion of current Data Protection and Freedom of Information related issues and provides invaluable cross-sector networking opportunities. It encourages cooperation between organisations in all sectors, and aims to complement the efforts of existing sector specific associations to provide a

strong unified voice for professionals in this dynamic environment.

The Data Protection Forum provides a focus for all sectors on the exchange, analysis and communication of information on Data Protection and Freedom of Information law.

This response does not relate to any processing of personal data carried out by the Forum itself, but is a reflection of views obtained from the Forum's members.

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.

Comments:

For society:

Sharing personal information with and within the public sector can, if done properly and appropriately, improve the integrity and efficiency of public services, and aid the prevention and detection of crime. Examples of this include the use of systems such as the congestion charging system in the detection of crime, and could also include the ability for medical records to be passed to the appropriate care givers.

Sharing personal information within the private sector is a different issue. Personal information has a high economic value in this information age. Sharing personal information between UK organisations may therefore clearly have an economic benefit.

The private sector can also benefit from the ability to share information for the prevention and detection of fraud, and this is particularly key in the insurance and financial services sectors.

For individuals:

The benefits are less clear for individuals, but an efficient public service can result in a more convenient service and potentially enable individuals to obtain the correct service at an appropriate time and place. This also facilitates services such as purchasing road tax online, which makes use of DVLA databases, insurance databases, MOT databases etc, and results in a net benefit to the individual.

Convenience is also the key benefit of sharing information in the private sector, and this most often occurs where there are a number of service providers providing what appears to the consumer to be one service – such as a pharmacy obtaining information about repeat prescriptions from a local doctors' surgery to ease the collection by the individual, or insurance companies being able to share information regarding claims.

This type of sharing of information can avoid the necessity of individuals having to verify their identity on repeated occasions and repeat information to service providers in either the public or private sectors.

Question 3. What in your view are the key risks of sharing personal information to a) individuals and b) society? Please provide examples.

Comments:

For society:

The key risks include:

1. Erosion of privacy, or the right to a private life, where data sharing becomes so common that it is a required part of engaging in society.
2. Erosion of trust where systems are seen to be flawed and subject to either accidental misuse or fraud. This may then lead to a reticence towards providing personal information.
3. Creation of a society where personal information is requested to carry out transactions where it is unnecessary or disproportionate.
4. Creation of a society where individuals feel that they have lost control over their personal information and its destination/longevity.

For individuals:

The key risks include:

1. As above, as such risks impact on an individual level.
2. Increased risk of identity theft, as personal information becomes more valuable.
3. Increased impact of identity theft. Where personal information is widely shared, it is often then used as an identifier. Whilst a lost or stolen password can be reset or changed, stolen personal information will still be in use by the individual.
4. Use of inaccurate or incomplete personal information which is obtained from sources other than the individual.
5. Use of inappropriate personal information, collected for specific and different purposes, where personal information is shared too widely.

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, pose the greatest opportunities or risks? Please explain the reasoning behind your response.

Comments:

The greatest opportunities lie in the ability to make government (and potentially other) services more accessible and convenient to individuals in society. There is clearly a great

opportunity in sharing information to allow transactions to occur easily and seamlessly online.

The greatest risks lie in the security of such systems and their potential reach, together with a lack of information - and more importantly information that the individual impacted understands. This is therefore all the more evident in cases where information is collected by necessity or under law, for example tax information, criminal records information (including DNA), as such systems are not subject to any consent regime.

It should always be remembered that just because information can be collected, processed and shared does not mean that it should be or that it is appropriate for it to be.

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.

Comments:

We have insufficient information to answer this question, and that is perhaps of concern. There is a general ignorance, and mis-information, about the level of personal information collected by public authorities and what it is used for.

It would be interesting to know whether public authorities are consistently implementing data retention (and moreover destruction) policies. It seems from press coverage around how long police records are kept for, for example, that this has not been consistent historically.

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.

Comments:

There appears to be an increase in the practice of private sector organisations requesting excessive information before a service or product can be purchased, for example taking names and addresses at the point of sale in store, or in online transactions requiring “market research” type questions to be answered before the transaction can proceed.

This is not per se an issue with the information held by the organisation, but regarding the fact that individuals are not given the opportunity to refuse to provide the excessive information other than to stop the transaction at that point. They are not necessarily provided with sufficient information about how this information will then be used.

There is also a general reticence within organisations to implementing data retention (and moreover destruction) policies, and as a result personal information is frequently held too long. This perhaps has two sources – the complex rules regarding how long different types of information must be kept, and the ever reducing price of electronic storage capacity.

Some private sector organisations, again in the insurance and financial services sectors specifically, may not have access to all the information they require in order to adequately

carry out their investigations into, for example, fraud.

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 not being shared, detailing what the barriers to the sharing of personal information are – e.g. legal, cultural, financial, institutional – and how these barriers can be overcome...

Comments:

A respondent from the insurance sector has suggested that information such as “no claims history” should not be subject to administrative burdens caused by the DPA, particularly where individuals are keen for this information to be shared.

Otherwise, no examples were given.

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.

Comments:

Again, it is very difficult from an external perspective to know when and how personal information is being shared and therefore to provide valuable comment on this. There is a perception that too much information is collected and shared both in the public and private sectors. It does seem, from anecdotal evidence, that for example the police are able in practice to obtain much more information than would seem possible under the Act and police powers, simply by the power of asking – the ostensible authority of the police and other public authorities should not be underestimated and individuals and private sector organisations are often given the impression that they are required to provide information to such authorities.

One member of the forum has commented on the difficulties which arise when two service providers are involved in the provision of a service to an individual and appear to be “joint data controllers”. It is not always clear what sharing of information needs to occur in this instance, and the applicable responsibilities of each data controller.

Another member commented on the ease of sharing personal information with data processors, particularly those based outside the EEA. Whilst the Act requires the data controller to take responsibility for this information and the reliability of its processors, in particular the model clauses seem to be seen as simply an administration exercise and do not in fact provide significant additional protection to individuals (particularly as individuals are almost certainly unaware of the transfer).

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.

Comments:

The Act is a complex piece of legislation, but which in practice boils down to some simple concepts of protection of data. However, this simpler view is almost never seen by the public or by organisations who struggle with the various concepts which provide (by necessity) many grey areas and few hard and fast rules.

However, even if the Act was simple to understand and apply, it can appear that there is little reason for some data controllers to comply with the Act as in practice a failure to comply is rarely met with a significant consequence. The recent media coverage of this issue has however reinforced the threat of 'naming and shaming' in the national press which has been used to good effect in the past. Organisations who are regulated by other regulators such as the FSA may also suffer financial penalties, albeit such consequences will not apply equally to all data controllers.

It is of concern to members of the forum that government and the courts, perhaps until recently, have paid little notice to the Act. Employment tribunals, for example (and again anecdotally), often overlook the fact that evidence may have been obtained in contravention of the Act.

We would make clear that, particularly in recent times, the profile of the Act is high in the UK, and individuals are becoming more aware that they have rights, even if they don't always understand what they are. However, misinformation, often given inadvertently by well-meaning service providers ("I'm afraid I can't tell you that because of data protection..."), does not always help the cause.

Jargon

The language or jargon of data protection could benefit from being brought up to date. Without wishing to be brought into the debate on what constitutes personal data (although it is clear that we still need clarification regarding what information falls under the Act following *Durant* and the guidance produced by the Article 29 working party and ICO), concepts such as "relevant filing system" simply either allow data controllers who are that way inclined to enter into technical debates as to why their data is not caught, or confuse other data controllers who are unsure what information they should be seeking to protect.

The issue is not one of the nature of storing the information, but of the impact of a misuse of that information.

The Principles

The data protection principles are key to the Act, but they themselves could be simplified. In particular, the first principle overarches all of the others. It requires that certain information be provided, including the purpose for the processing of the data – which could be argued

makes principle 2 redundant. There are certain types of processing that individuals are aware must occur for a particular transaction to take place and do not want to listen or read long statements explaining what processing is going to occur.

There is not always a clear distinction in the eyes of organisations between those areas where a controller must provide information (guidance to first principle) and those areas where it must obtain consent (schedules 2 and 3).

The conditions for processing are in themselves sensible (although query why there is not a clear-cut condition for processing non-sensitive personal data for the purposes of legal proceedings), but the language is not. Businesses do not understand that they need “a condition for processing”. Rolling this requirement into principle 1 simply adds confusion and takes the focus away from the fairness of the processing.

Subject Access Requests

Subject Access is another area of difficulty for businesses (particularly in light of the debate around what are personal data and a relevant filing system). Of particular concern on one side is the disproportionate cost that a DSAR may result in, and the £10 fee payable; on the other side is a perceived lack of enforcement where DSARs are not handled properly and a reticence of individuals to exercise this right unless pushed to do so for the purposes of litigation or employment complaints. Also often misunderstood is the fact that not only does a DSAR give the individual the right to obtain copies of information, but also a right to know to whom the information is disclosed, and where it came from. From experience, it seems that this information is rarely provided, possibly because the data subjects themselves are unaware of this element of their rights.

Sanctions

There is a key issue around the funding and powers granted to the Information Commissioner’s Office. If the Act is to have any effect at all, it is vital that the regulator is adequately resourced to provide assistance, guidance, and perhaps more importantly, enforcement.

Once such resources are available, there must be effective sanctions. However, the approach of the ICO of working with business to generate a culture of compliance is still required – it just needs a consequence if that culture is not maintained.

As the Act is not a simple, rule based, tick box exercise, the enforcement of it cannot be either, and negotiation, education and care must be taken to ensure that organisations are not penalised simply for falling too far over the faint grey line. However, clear breaches or disregard for the principles of the Act should be dealt with firmly.

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.

Comments:

Anecdotal evidence suggests that there is a mixture in compliance. Whilst organisations do try to comply, there is a feeling that the obligations to provide exhaustive details of how personal information is to be processed does not always fit within business models and can be very restrictive. It is very hard to maintain customer databases which make note of what information was given to each contact at the time their information was obtained, and as such businesses find it difficult to update their fair processing notices and keep track of what they are able to do with the information that they collect.

Despite these endeavours, fair processing notices are often poor, and only considered when a new activity, such as a new website, is contemplated, rather than at all points of personal information collection. Notices are often complex and difficult for consumers to understand, as businesses are trying hard to consider what they may wish to use personal information for at some undisclosed date in the future.

In relation to service provision, however, this is rarely problematic. The major area where this is an issue is in the use of personal information for marketing purposes.

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

Comments:

Legacy IT and other organisational systems are a key issue, because of the cost of changing them and the fact that they were not designed with data protection in mind.

On the other hand, new technologies also pose problems. The prevalence of digital data means that data controllers are dealing with information which many individuals would not understand existed or was tracked, including metadata. The low cost of data storage means that personal information may be held for longer than necessary, because it can be without additional expenditure. New technologies which allow the manipulation and promulgation of information mean that even more information is available easily and economically – but does that mean it should be processed?

Within organisations, different positions have different views on this matter, and where such exploitation can mean a business gain, there is a strong desire to focus on that, rather than consider data protection at an early stage in designing the product.

There are a number of misunderstandings of the legislation, ranging from individuals who either believe that nothing can be done with their information without their consent, or that the legislation will do nothing to protect their information; to organisations who see the Act as an unnecessary fetter on their business activities and therefore don't comply, or those who comply to the letter but not the spirit, resulting in press coverage blaming the Act for the actions of utilities failing to inform social services when they cut off pensioners, or the police not retaining records of past offenders who offend again. It need be none of these things!

The fact that failure to comply with the legislation can appear more economical to data controllers than compliance will continue to be a problem until either penalties increase or individuals insist on compliance with the Act from their service providers.

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

Comments:

Additional enforcement powers are clearly required. However, which enforcement powers are appropriate will need to be carefully researched. The following should be considered:

1. Introduction of the promised custodial sentence for breach of s55 (and potential expansion of the offence to cover knowing or reckless abuses of personal data made with the consent of the data controller).
2. ICO to be granted powers to fine those who breach the Act directly rather than waiting for court action.
3. Maximum fines to be increased.
4. Additional guidance to be given to courts who must consider data protection as and when it arises – ICO guidance to be binding.
5. Audit (without notice) rights to the ICO.
6. Introduction of a data breach notification requirement.
7. Requirement for organisations to appoint a data protection officer, along similar lines as FSA approved persons.

If any of these additional powers are to be introduced and become effective, the ICO will require significant further funding. One consideration for this may be to look at the notification system and fees, which are currently indiscriminate relating to the amount of personal information, processed, and could be increased on a sliding scale.

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.

Comments:

One member of the forum has suggested that the Access to Medical Reports Act which allows an individual to access a medical report before submission to an insurer EC45/2001, applies a good approach to this problem.

There is a clear overlap in the financial services sector between regulation carried out by the FSA and the ICO, and the FSA has shown its superior enforcement powers in recent cases. Sector specific regulation is the backbone of data protection in the US, and there may be a place for some sector specific regulation in the UK, as there are clearly particular issues in particular sectors (financial, insurance, children, health, marketing). Where there is existing legislation in this area, it can be confusing for organisations to understand which legislation

plays the trump card.

There is a concern that whilst the Act and the Directive are deliberately technologically neutral, they are failing to keep pace with developments in why data is being processed, rather than how. The reliance of the definitions on the manner of processing misses the current issues which tend to focus on the purpose of the processing.

The introduction of the Freedom of Information Act in the public sector has raised awareness of the regulation of personal data as well as non-personal data, due to the interaction of the two pieces of legislation, and this is to be welcomed. However, the differences between these two pieces of legislation (exemptions, time frames, fees) can cause great difficulties for public authorities who often have to deal with one request under 2 separate pieces of legislation.

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.

Comments:

Many organisations are unclear as to how they can verify that a request for information from a public authority such as the police, HMRC etc, is authentic and validly made. This has two issues – they need to be able to authenticate that the request truly came from the organisation in question, and then they need to be able to verify whether the organisation has the powers to request the information.

Linked to this is the need for insurance companies to share information with intelligence agencies to detect fraud committed by means of sophisticated organised crime since review on a case-by-case basis does not bring these instances to light. S29 would need to be enhanced, possibly on an industry specific basis to allow this to take place.

Regarding data sharing within the public sector, one suggestion is that such issues should be dictated by the information which needs to be shared. This could be identified in the course of a privacy impact assessment, and rules governing that type of sharing to be approved by the ICO who can maintain a register of such data sharing.

As outlined above in relation to “joint data controllers”, a further issue to be considered is the rights, responsibilities and roles of the people involved, who is the owner, and who is the custodian, the guardian, the agent of the data, and who is responsible for data content and quality. Clarity is needed on the different types of responsibility, and where the boundaries lie (though these are subject to change).

It is clear from recent experiences that if large amounts of data are to be shared and transferred, clear legislation is required around the area of ensuring the security of data, including firmer guidance around the seventh principle.

Outsourcing is now a run of the mill undertaking for many businesses. As a common activity, it may, for example, be appropriate to reintroduce the concept from the 1984 Act that a data controller's agent was in essence the same as the data controller, therefore allowing the data controller to pass information to their data processor without concern.

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.

Comments:

The following comments do not necessarily fall into the heading of "unreasonable burdens", but are problems that organisations face when trying to comply with the Act.

Conditions for processing sensitive personal information

Schedule 3 conditions for handling sensitive data causes frequent problems for many organisations where there is no clear Schedule 3 condition and consent must be sought. The ICO has in some way acknowledged this in the Employment Practices Code, where it is acknowledged that even handling employee sickness records does not clearly fit within one of the conditions, but clearly must take place.

There is often a situation where the processing is in the interests of the data subject (although not necessarily in their vital interests), but where consent is required to be sought and recorded, and these processes and systems place a burden on businesses.

Subject Access Requests

Subject Access Requests can also be an area where there is a disproportionate burden on organisations. The costs implications of carrying out searches should be reflected either in the fee structure or the obligation. Whilst computerised records may in principle be searchable, this is not always in practice the case; and in any event a computer is unable to determine what personal information is in the context of the Act.

Notification

Notification as it currently stands is an administrative burden, but one which provides no real benefit to the individual or the regulator. If notification is to remain, it should provide the ICO with real information as to how organisations process data and be a starting point for any audit. The fee structure for notification could be used as an opportunity to fund the regulation of this area, but also to ensure that organisations who wish to carry on significant data processing outside of exempted purposes have taken the cost of data protection compliance into account in their business plan. Another suggestion has been to be able to deal with notification and data protection compliance at a group level. Administratively, this would solve many issues for large organisations, and may also permit the free transfer of data within these organisations.

Handing professional contact details

Another difficulty is in relation to whether all obligations under the Act apply when organisations are simply handling the contact details of individuals in a professional context. This does not seem to be clear cut.

Section 4: Consent and transparency

Question 16. Is it clear whether and when you need individuals' 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.

Comments:

No, it is not clear when consent is required or what form consent should take. (See also our response in relation to principle 2 above). The mix of terminology used – consent, informed consent, implied consent, opt-in, opt-out, soft opt-in – all add to problems in knowing when an individual simply needs to be informed of the processing which is taking place, or needs to indicate that they have accepted it. It is also not clear the extent to which a service can be refused if consent is not provided.

There are many further issues relating to consent regarding whether it endures, whether it can be revoked? If so, how does an individual revoke consent for sharing where he/she may not be sure of the legal entities with whom the information has been shared. Are there obligations on the original data controller to ensure that such revocation is communicated on?

In addition to revoking consent, it may sometimes be in the interests of different data subjects to withhold consent (and thereby disclosure) rather than give consent for disclosure for example in road traffic accident insurance claims. There is no method to balance such discrepancy and the rights of each individual. It is often thought that the Act allows a right of access; whereas in fact, the exemptions only provide a reason why disclosure is not prohibited, rather than a power to force disclosure.

Question 17. What, if any, barriers would a requirement for gaining consent create to the sharing of personal information? Please explain your reasoning.

Comments:

Often the difficulty comes after a relationship has started, when something changes - desire to move business to another data controller, use of different anti-fraud databases, desire to market customers. The cost involved with contacting customers specifically is very high and then people don't write back. Then what do you do with the people who didn't 'consent'?

This can also be true if new statutory obligations are imposed upon the Data Controller.

Many individuals when faced with requests for consent contained in terms and conditions, privacy policies or fair processing notices do not read or understand what they are consenting to, and often the consents requested are so wide that the individual has no way of controlling the future promulgation of their data, other than to refuse to take on the service. Individuals have very little negotiation power, and so if the consent process is to be

improved, there must be an obligation, incentive and guidance for service providers to make this process simpler and easier.

However, consent and information are key protections with regard to privacy and should not be overlooked simply because in some cases they can be difficult. Guidance from the ICO on if and when implied consent can be used and the length of time individuals should be allowed to object within would be practically very useful.

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 and sharing of personal information to the public? And if so, how?

Comments:

Data controllers should be required, encouraged and helped to make fair processing notice readable and not too long.

There was also a suggestion that industry wide fair processing notices could be given, so that individuals are given assurances of consistency. For example, in the insurance industry there could be a joint statement by insurance companies which describes how the insurance industry uses and shares data, including fraud prevention, sharing with the police etc. This could be held on the ABI website and on request from a company. This could then be augmented if additional processing was taking place.

If notification is to remain, a clearer and more accessible notification system may benefit transparency.

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)?

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

Comments:

Privacy Impact Assessments are very valuable in designing systems which at the outset are made to take privacy into consideration. However, without any obligations on data controllers to use such systems, it will be hard to assess their uptake and effect. However, anecdotally, many data protection officers found the announcement of PIAs to assist in obtaining "buy-in" from their business partners.

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.

Comments:

It seems clear that technological advances have made the sharing of personal information much easier. It has also made the manipulation and the business benefits of sharing information more economical and the opportunities seem endless. However, whilst technologies for the protection of personal information are available, they do not provide the same business benefits and are not being used as widely.

The value of the data and the portability of the data unfortunately make for an unwelcome attraction to those who wish to abuse it.

The increased ability of workers to work from home and to use their own IT equipment in their business life has also lead to potential security breaches. Much education needs to take place at an individual level, as almost all members of organisations have access to personal information, not only those higher level employees who may otherwise have been trained in the Act.

However, technological advances also provide more opportunities to provide this training and awareness through company intranets etc.

Question 21. Should the law mandate specific 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?

Comments:

There are a number of problems with the law specifying the technical safeguards:

1. technology is developed very quickly and therefore the law would be always chasing technology
2. in the window where the law does not specify the right technology to use, and there is a breach, would the Data Controller be absolved of blame?
3. when the public's attention is taken away from this topic, would parliament be less concerned to update the technology to be used?

However, the law could mandate risk management and document management procedures which are technologically neutral, but which ensure that technology changes are protected with robust security mechanisms.

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?

Comments:

Anonymisation is an area of interest to many data controllers, but there is insufficient guidance as to how this can be done and the responsibilities which remain once information has been anonymised. For example, outside of particular sectors, it is not well understood how information can be severed from personal information so that the two can no longer be assimilated, as otherwise the definition of personal data will still apply (as that information, together with other information held by the data controller would still relate to an identified individual).

Aside from lack of understanding, a further barrier to these technologies is the cost of implementing them.

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.

Comments: Other than general comments with regard to other European regimes and the data breach notification and sector specific regimes in the USA, we have no specific knowledge.

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?

Comments: No response

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?

Comments: No response

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.

Comments: No response

Section 7: Additional questions

Question 27. 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.

Comments: No response

Question 28. 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?

Comments:

This consultation covers a very wide range of issues. The comments made in this response are therefore not exhaustive comments in relation to the issue of protection of personal information or indeed the individual questions raised in the consultation. The wide remit of the consultation has possibly, unfortunately, deterred some interested parties from submitting focussed responses.

The members of the Forum would be glad to enter into discussions on a whole range of areas in relation to data protection.