

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

15 February 2008

Direct Line: 020 7951 4965
e-mail: gwatkins@uk.ey.com

Dear Sirs

Draft Data Sharing Review Consultation Paper, February 2008

INTRODUCTION

1. Ernst & Young LLP is grateful for the opportunity to comment on the questions posed in relation to data sharing in the UK.
2. We recognise the importance of this paper and welcome the decision to undertake an exercise to gather both public and private sector input on data sharing. We hope that we will get the chance to review the results of this paper and would welcome the opportunity to provide input on any proposed changes to the legal framework that arise from the responses to this paper.
3. We have noted below our key observations and have answered the questions in the consultation paper, within the context of our overarching requirement to ensure that we uphold our client confidentiality obligations. We have not submitted a response to questions where there is a risk that our response may be attributable to our clients.
4. We have included detailed comments on specific aspects of the draft in the attached response template as requested, for clarity and ease of reference.

OVERALL OBSERVATIONS

5. We recognise the ever increasing importance of data sharing within developed markets across the world and the associated savings and benefits that may be derived.
6. Further protection and enforcement measures could be beneficial, including: enhanced notice and consent requirements; more controls on the flow and use of data; tighter monitoring and auditing powers; stricter 'breach notification' procedures; and greater legal and fiscal penalties. However, these would all need to be carefully considered with a detailed analysis and assessment of the need to balance the benefits of greater protection and control against the potential financial and economic costs of compliance and potentially negative impact on individuals, commerce and society.



INVESTOR IN PEOPLE

7. It is our considered view that as companies, governments and individuals seek to share ever growing levels of personal data, the laws and regulations that govern the sharing of this data are becoming widely recognised as a key method for helping to protect individuals' rights in the global economy. We believe it is important that legislators consider the practical implications of the legislation they are proposing, to help ensure that whilst individuals may be adequately protected, it should not be at a level that curtails the competitiveness of the economy in which the companies that may be required to comply with the legislation operate.
8. The current UK DPA legislation is principles-based, which allows businesses to interpret its requirements in the context of their own particular business circumstances and respond appropriately. On balance our view is that the principles enshrined within the UK DPA are not unreasonable at the current time given the need to protect and maintain the rights of individuals.
9. From a societal perspective, we are not convinced the impacts of ineffective control over and inappropriate use of personal data are well enough understood by the general population. If they were, then there might be greater expectations and pressure from the population on companies to implement effective controls and a greater awareness and feeling of responsibility amongst individual employees (as citizens themselves) to consider data protection issues in performing their job roles and function.
10. New technologies keep introducing new opportunities for protecting and exposing personal data. Yet, technologies such as e-mail, CD, and archiving media, which are no longer considered novel, have contributed as a leading factor in the inappropriate protection and sharing of personal data. Some of this is inevitably down to a lack of awareness of individuals of the risk associated with processing, storing, and sharing personal data, rather than the particular technologies used to do so. Upfront user awareness campaigns should therefore form a key part of the launch of new data collection / sharing / storage technologies and techniques.
11. We hope our views, in this letter and in our response, are helpful. If you would like further clarification on any of the points raised please contact me. We wish you every success with this consultation and look forward to participating in this process going forward.

Yours faithfully

Giles Watkins
Partner
Technology and Security Risk Services

	Questions	Our Answers
Q1.	<p>Q1. Please explain what your interest in data sharing is.</p> <p>If you have an active involvement in personal data sharing, we would be grateful for the following information:</p> <ul style="list-style-type: none"> • What kinds of personal data 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? 	<p>Our involvement in data sharing falls into four broad categories:</p> <ul style="list-style-type: none"> • as an employer we collect, store and process personal data (on current, future and former employees) in a way that is compliant with the UK’s Data Protection Act and, where appropriate, regulations in other jurisdictions • a mix of specialist teams who will, from time-to-time, as instructed by our client, collect (via most transfer methods), store (electronically and physically) and process client data that relates to individuals (e.g. employment contracts, performance records, and payroll) • a professional services firm (audit, assurance, risk, tax, transactions and business advisory) that advises organisations and companies across business sectors and jurisdictions around the globe • professional services network of firms, advising international clients and sharing data on those clients across relevant parts of the network at a corporate, organisational and/or individual level. <p>We are aware of our responsibilities in relation to this data, which we communicate to our staff through various mechanisms including internal policies and procedures, which are readily available to all staff. These are supported by technical and process controls to help ensure that we collect, use and retain personal data strictly in accordance with our legal obligations e.g. access is restricted to individuals who require it, with the appropriate degree of authorisation from those to whom the personal data relates.</p>
Q2.	<p>Q2. What in your view are the key benefits of sharing personal data to a) individuals and b) society? Please provide examples.</p>	<p>a) We believe the key benefits to individuals include the:</p> <ul style="list-style-type: none"> • ability to access and/or receive “personal” products and services e.g. banking and credit facilities; insurance; travel; leisure; health care; education; social security; legal support and police assistance • opportunity to consume products and services, from commercial and public sectors, which are tailored



		<p>to our specific needs at a time, quality and cost appropriate for our requirements and / or means</p> <ul style="list-style-type: none"> • opportunities for employers to support the personal and career development opportunities of their employees. <p>b) We believe the benefits to society include:</p> <ul style="list-style-type: none"> • the formulation, implementation and enforcement of effective economic, social and financial policies by central and local government • new and enhanced products and services developed from intelligence gathered on the attitudes and behaviours of individual consumers • advancements in medical science, with an associated increase in the health and longevity of the population, and a corresponding decrease in the cost of medical and other care services • greater surveillance of citizens to support the prevention, detection and prosecution of criminal and terrorist activities • for many organisations, the sharing of personal data in a controlled manner is a core business need in delivering their services in a competitive and efficient manner.
Q3.	Q3. What in your view are the key risks of sharing personal data to a) individuals and b) society? Please provide examples.	<p>a) In our view the key risk with sharing personal data is the unauthorised disclosure, access or theft of the component parts of a person’s personal identity. The associated risks and consequences will apply to the individual whose data is misappropriated and the individual or entity that lost it (in part or whole), or failed to prevent unauthorised access to it (in part or whole) while the data was stored, communicated and/or conveyed by some other means/third party. In addition, the “stolen” or “lost” identity may be used against the individual owner or someone else for criminal gain.</p>



		<p>Furthermore, whilst an individual’s identity may not be stolen as a consequence of lost or stolen data, the lost data may enable individuals to infer data, such as behavioural activity (e.g. buying patterns) which individuals may not wish to become public.</p> <p>The consequences for the individual whose data has been compromised will obviously depend on:</p> <ul style="list-style-type: none"> • the quantity and quality of the data • whether the loss and/or misappropriation was accidental or perpetrated with a criminal intent • their awareness of the loss and ability to take remedial action to stop or limit unauthorised use of the data (e.g. to acquire goods and services). <p>b) In our view the key risk for society, when personal data is lost or misused, is the ability for criminals to organise and/or commit (in some cases remotely from other jurisdictions) crimes against large groups of individuals. Further privation may arise for the victims and others indirectly, as:</p> <ul style="list-style-type: none"> • banks and insurers cover these losses and potential risks with higher premiums • governments add more complexity and cost to those who use and manage personal data with ill-conceived regulation • security agencies increase the intensity of their surveillance on the lives of innocent citizens.
Q4.	Q4. As mentioned in the introduction, there are wide variations in the scope and methods of personal data sharing. What scope and what methods, in your view,	In relation to “scope”, the most significant risks may arise where personal data is shared outside well defined organisational and/or geographical boundaries, and where the data shared is excessive for its intended use. In these circumstances the greatest risk of unauthorised access and/or misuse is likely to occur, because personal data may be exposed to unauthorised individuals and/or individuals who may not fully appreciate



	<p>pose the greatest opportunities or risks? Please explain the reasoning behind your response.</p>	<p>its sensitivity and hence the level of protection it should be afforded.</p> <p>In terms of “methods”, the greatest risks lie in the use of mechanisms and/or media that might allow the data to be inappropriately disclosed to unauthorised individuals, either intentionally or accidentally. For example, transporting sensitive personal data using unsecured physical files, or unencrypted disks, USB memory ‘sticks’ or emails.</p> <p>There are undoubtedly opportunities to utilise technical measures (e.g. encryption and other logical access controls) to reduce many of the risks associated with sharing personal data. However, the application of these is often dependent upon a high level of awareness in individuals of the sensitivity of the data they are sharing and processing. Therefore the risks and opportunities will be relative to what is held, by whom, and for what purpose.</p> <p>The increased use of techniques, such as training and awareness campaigns and data classification schemes, may also present opportunities to manage more effectively the risks associated with sharing personal data. However, these opportunities need to be considered in light of the difficulty and cost of their implementation and use.</p> <p>Moving data across borders may change the associated risks as the requirements placed on data may change.</p>
Q5.	<p>Q5. 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.</p>	<p>In our view it is difficult to say, with any degree of accuracy, whether a public authority holds too much or too little data. For this reason we prefer not to comment on this matter.</p>
Q6.	<p>Q6. Please provide examples of where, in your view, private sector organisations hold too much personal data or not enough personal information, and the reasoning behind your response.</p>	<p>In our view it is difficult to say, with any degree of accuracy, whether a particular category of private sector organisation holds too much or too little data. For this reason we prefer not to comment on this matter.</p>



<p>Q7.</p>	<p>Q7. Please provide examples of cases where you believe the sharing of personal data between two or more bodies would be beneficial, but where it is not currently taking place. Please explain as fully as possible why data is not being shared, detailing what the barriers to the sharing of personal data are – e.g. legal, cultural, financial, institutional – and how these barriers can be overcome.</p>	<p>According to recent press reports on alleged failures across “social welfare” services, it seems that the collation, storage, and shared access of individual case files needs to be improved. One key concern is the apparent fact that the various agencies implicated in these “alleged failures” (e.g. police, social services, probation services, GPs and hospitals) appeared not to have the means to identify quickly accurate records on suspected abuse victims. In our view it is difficult to say, with any degree of accuracy, instances of where personal data should not be shared between two or more bodies. For this reason we prefer not to comment on this matter.</p>
<p>Q8.</p>	<p>Q8. Please provide examples of cases where you believe that personal data 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.</p>	<p>In our view it is difficult to say, with any degree of accuracy, instances of where personal data should not be shared between two or more bodies. For this reason we prefer not to comment on this matter.</p>
<p>Q9.</p>	<p>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 manner incompatible with that purpose or</p>	<p>In our view the DPA achieves its purpose by defining personal data and clarifying the responsibilities of those who use it.</p> <p>Some of the specific strengths and weaknesses that we see with the DPA are as follows:</p> <p>Strengths</p> <ul style="list-style-type: none"> • it is in line with Generally Accepted Privacy Principles and the European Data Protection Directive, which helps to standardise and simplify requirements for data controllers and processors. This helps to reduce the cost and complexity involved with compliance and, in turn, increases the likelihood of



<p>those purposes.” Q9. In your view, how well does the DPA work? Please outline the DPA’s main strengths and weaknesses and proposals for changes you would like to see made, including suggestions for their implementation.</p>	<p>effective implementation</p> <ul style="list-style-type: none"> • it makes provisions to ensure the use of personal data is transparent to the individuals to which it relates • it is ‘principles-based’, which allows scope for interpretation and the development of processes and procedures that are ‘fit for purpose’, depending upon specific circumstances and risks, rather than imposing ‘one-size-fits-all’ rules that may be cumbersome or unrealistic to implement • it focuses on, and protects the rights of, individuals eg, by providing individuals with the right of access to data that relates to them. <p>Other areas what we considered as strengths include:</p> <ul style="list-style-type: none"> • cross-regulator working (e.g. Information Commissioner and the FSA) • the evolution of a data protection framework • the use and development of supporting tools (e.g. privacy impact assessment). <p>Weaknesses</p> <p>There are opportunities to enhance an individual’s level of awareness and understanding of the implications of the consent they provide, specifically: the sensitivity of the data; how it will be used; when; by whom; and for how long.</p> <ul style="list-style-type: none"> • the effects of the DPA - creating appropriate behaviours for data providers and users - depend on how it is enforced, • further protection and enforcement measures could be beneficial, including: enhanced notice and
--	---



		<p>consent requirements; more controls on the flow and use of data; tighter monitoring and auditing powers; stricter ‘breach notification’ procedures; and greater legal and fiscal penalties. However, these would all need to be carefully considered with a detailed analysis and assessment of the need to balance the benefits of greater protection and control, against the potential financial and economic costs of compliance and potentially negative effects on individuals, commerce and society.</p>
<p>Q10.</p>	<p>Q10. 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.</p>	<p>Our view is that the second principle is well intended, specifically in that:</p> <ul style="list-style-type: none"> • individuals should have the right to provide data for specific purposes only • it aims to provide the public with confidence that the organisations holding their personal data can be trusted. <p>We do not believe there is extensive or systematic abuse of the second principle. However, the increasing complexity of organisations, and the information systems they use, means that data may be transmitted to and stored in many places, potentially making it available to a wide audience. The greatest risk of non-compliance with the second principle would seem to be through: individuals’ lack of awareness of the sensitivity of the data they may be accessing; the specific requirements of the DPA and the purposes for which the data was originally collected; in addition to individuals understanding of privacy notices (e.g. opt-in or opt-out). This may result in individuals within organisations using personal data for seemingly valid and beneficial purposes, but unwittingly breaching the original notice or consent conditions.</p>
<p>Q11.</p>	<p>Q11. What technical, institutional or societal barriers stand in the way of the effectiveness of the DPA? Please provide examples.</p>	<ul style="list-style-type: none"> • Some of the technical solutions can be prohibitively expensive when considered in the context of current legislative penalties resulting from a breach. For example, the lack of effective data architecture within many organisations may lead to the unknown or poorly controlled collection, use, disclosure and/or retention of personal data.



		<ul style="list-style-type: none"> • Consideration of other potential factors, such as reputational impact and loss of consumer, customer and stakeholder confidence, may make the case more compelling. • We are not convinced that the issues and effects of the DPA are fully understood by the general public. If they were, there might be more pressure on the users of personal data to implement effective controls more consistently. There may be various ways to educate the public on this matter, but the associated costs and benefits of doing this would need to be considered very carefully.
Q12.	Q12. What further powers, safeguards, sanctions or provisions do you believe should be included in the DPA.	<p>As per our answer to questions 9:</p> <ul style="list-style-type: none"> • Further protection and enforcement measures could be beneficial, including: enhanced notice and consent requirements; more controls on the flow and use of data; tighter monitoring and auditing powers; stricter 'breach notification' procedures; and greater legal and fiscal penalties. However, these would all need to be carefully considered with a detailed analysis and assessment of the need to balance the benefits of greater protection and control against the potential financial and economic costs of compliance and potentially negative impact on individuals, commerce and society.
Q13.	Q13. 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.	<p>We are not aware of specific instances where other aspects of UK law or EU directives affect (positively or negatively) data sharing or data protection. There are, however, future legislative provisions that may need to be considered in the context of data sharing and protection, for example anti-terrorism and crime prevention/detection, financial services and taxation.</p>
Q14	Q14. Are there statutory powers unavailable that would enable better and more secure sharing of personal information– for example for identity authentication purposes – between a)	<p>As per our answer to questions 9:</p> <ul style="list-style-type: none"> • Further protection and enforcement measures could be beneficial, including: enhanced notice and consent requirements; more controls on the flow and use of data; tighter monitoring and auditing powers; stricter 'breach notification' procedures; and greater legal and fiscal penalties. However, these would all need



	<p>public authorities and b) public authorities and private organisations? If so, what are they? Please provide examples and steps you believe could be taken to improve matters.</p>	<p>to be carefully considered with a detailed analysis and assessment of the need to balance the benefits of greater protection and control against the potential financial and economic costs of compliance and potentially negative impact on individuals, commerce and society.</p>
Q15	<p>Q15. 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.</p>	<p>The current UK DPA legislation is principles-based, which allows businesses to interpret its requirements in the context of their own particular circumstances. In our view this flexibility should help to ensure the DPA retains its applicability to the varied use of data sharing. This seems like a reasonable way forward, although we accept that “reasonableness” will depend on the views of each and every user of personal data.</p> <p>If or when refinements are made to the current legal framework, regulators may consider using either definitive rules or principles-based legislation. The advantage of definitive rules is that they can set out clearly the obligations on business and apply equally to all organisations. The advantage of principles-based regulations is that they provide more opportunities for businesses to assess the risks which <i>they</i> need to address, so <i>they</i> can respond accordingly.</p>
Q16	<p>Section 4: Consent and transparency Q16. Is it clear whether and when you need individuals’ consent to share data about them? Are you clear about the form that consent should take? Please provide examples. Please provide details of initiative you have been involved in that has been based on consent.</p>	<p>The requirement to gain consent is explicitly provided within the legislation. However, at present the consent notices provided by organisations can vary significantly, in form and sometimes content (e.g. opt-in or opt-out). Whilst they may be appropriate to meet the requirements of the legislation, they may not provide the data subject with sufficient clarity or a significant enough level of detail to adequately understand what they are consenting to.</p>
Q17.	<p>Q17. What, if any, barriers would a requirement for gaining consent create to</p>	<p>A formal requirement to gain consent in all circumstances would be likely to create additional costs to organisations. It may also result in unnecessarily cumbersome and confusing communication mechanisms</p>



	<p>the sharing of personal information? Please explain your reasoning.</p>	<p>with consumers and customers, through complex forms and registration processes (e.g. opt-in and opt-out). But again, this needs to be considered in the context of both making sure an individual is fully aware of what their personal data will be used for and by whom, as well as ensuring that the individual has the opportunity to ‘opt-out’ where appropriate.</p>
<p>Q18.</p>	<p>Q18. Do you have any suggestions on how to make the sharing of data 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 data to the public? And if so, how?</p>	<p>To enable greater transparency, policymakers may wish to consider the implementation of rules containing the minimum standards and guidelines required for privacy notices. If considered appropriate, the regulators should be encouraged to take a pragmatic approach to allow for greater transparency to be achieved, without putting unrealistic obligations on entities required to comply.</p>
<p>Q19.</p>	<p>Q19. How can we best ensure that data sharing policy is developed in a way that ensures proper transparency, scrutiny and accountability? For example: In your view, how valuable is the data Commissioner’s recently published Framework code of practice for sharing personal data (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 data Commissioner on 11 December (www.ico.gov.uk)?</p>	<p>In our view, the most appropriate means to develop effective data sharing policy is to:</p> <ul style="list-style-type: none"> • consult the public and business organisations in the UK and other jurisdictions, to map out and prioritise the issues that need to be managed • assess how other jurisdictions legislate on this matter, to determine the effectiveness or otherwise of different types and levels of regulation • determine whether, or to what extent, new or enhanced policy is the right way forward • consider other actions (guidance, education and training) which might complement or substitute legislation • conduct rigorous impact assessments, to focus the policymakers on the cost effectiveness of any proposed policy.

Q20.	<p>Q20. What impact in your view have technological advances had on the sharing and protection of personal information? Please provide examples.</p>	<p>Technological advances have made it easier (quicker, simpler, cheaper) to collect, process, and share large amounts of data globally. But as organisations and information systems become more complex and dispersed, along with bigger data flows, it is likely to become an increasingly difficult challenge for organisations to effectively manage the collection, use and retention of personal data.</p> <p>However, whilst new technologies (e.g. Mobile data storage devices such as smart cards as RFID tags, etc) introduce new opportunities and risks for protecting and exposing personal data, unless or until individuals become more aware of the risks, the current challenges associated with data sharing will persist. Upfront user awareness campaigns should, therefore, form a key part of the launch of new data collection / sharing / storage technologies / techniques.</p>
Q21.	<p>Q21. Should the law mandate specific technical safeguards for protecting personal information? For example, should there be an explicit requirement that personal data held on portable devices be encrypted to a particular standard?</p>	<p>The consideration and selection of mandated technical safeguards needs to assess the type of data being shared, when, where, by whom and with what means. For this reason it would be difficult to mandate a single technology or standard to cover all circumstance. It is also likely that any specific technology or standard chosen would need to be frequently updated to keep pace with general advances in technology, and the capability and sophistication of threats to personal data. Therefore, on balance, we do not believe it would be practicable for the government to mandate any specific technology.</p>
Q22.	<p>Q22. 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</p>	<p>Privacy enhancing techniques may be an element for consideration when seeking to identify safeguards for helping to protect an individual's privacy. In addition, if performed correctly, anonymised or "pseudo anonymised" data may be of significant value to entities performing such activities as medical research. However, it is important that careful consideration is given to the processes used and the purpose for which the data is held. In practice, many organisations have found that achieving an appropriate level of anonymisation or "pseudo anonymisation" is extremely difficult.</p>

	barriers to using them?	
Q23.	<p>Section 6: International comparisons Q 23.</p> <p>Are you aware of any jurisdictions whose legal framework for sharing and protecting personal data contains features that could be useful in a UK context? Please provide examples.</p>	
Q24.	<p>Q 24. Do you have any international examples of good practice in the sharing of personal data that could or should be adopted by the UK?</p>	
Q25.	<p>Q 25. Do you have knowledge of jurisdictions that have adopted a particularly permissive or restrictive approach to sharing personal information? What have the consequences of this been?</p>	
Q26.	<p>Q 26. Are you aware of significant differences in public attitudes to the sharing of personal data in other countries? Please provide examples and an explanation for why you believe this to be the case.</p>	



Q27.	Q 27. Are there any additional issues on the sharing of personal data and protection of personal data that this review should be considering? Do of these issues apply specifically to your sector?	
Q28.	Q 28. Please set out any additional suggestions or observations you have that you believe may be of assistance to the review.	There is an ongoing debate over the freedom and sharing of data and the right of the individual to privacy. Clearly, this is a critical balancing act. It is important that governments consider the practical implications of the legislation they propose, to help ensure that whilst individuals are adequately protected, such protection does not unnecessarily curtail the openness of society or competitiveness of the economy.