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.	
Comments:	EURIM brings together politicians, officials and industry in support of a globally competitive, socially inclusive and democratically accountable information society. Secure and appropriate information sharing is at the heart of the infrastructures that underpin the on-line world. EURIM has therefore been interested, from its inception, in the establishment of governance frameworks that recognise, promote and enforce good practice in the secure management of personal information and identities across the public, private and third sectors, particularly with regard to applications that cross organisational and sector boundaries.

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

Question 2.	
Comments:	a) Avoiding the necessity for individuals repeating the same information many times to different departments or agencies: joining up services for benefits, housing, health, education etc. underpinned by trusted and secure personal data treatment (including collection, storage and transmission as well as

access) with quality data.

b) Detection of and avoidance of terrorism and serious organised crime.

c) Improved customer segmentation so services can be more efficiently and cost effectively directed e.g. encouraging direct debit take-up for Council Tax payments through identification of target households.

d) the key benefits of sharing information to the citizen include single sign on to Government services and enabling customer-focused and proactive public services. This will save the citizen's time, speed up performance (e.g. more rapid benefits processing and delivery times), and improve trust. In the health arena, data sharing can provide timely and accurate data to faciltiate diagnosis and treatment, and can make the difference between life and death.

Examples include the 'Tell Us Once' programme developed and led by the DWP, where the primary objective is to look at introducing more efficient and effective processes surrounding the customer journey for birth and bereavement, as well as the creation of a Change of Address service by 2010.

e) facilitates joining up, thereby helping to avoid duplication, improving efficiency and savings. Data sharing also makes it easier for partnerships to detect, trace and combat crime, facilitates best practice and increases the ability of public sector organisations and service providers to support the most vulnerable in Society.

Information sharing would also reduce the need for business to provide the same data repeatedly to different public sector bodies, improving risk assessment, reducing costs and increasing competitiveness. At the same time, effective data sharing could help agencies ensure compliance..

Question 3.

Comments: Key risks of sharing personal information to (a) individuals include ID theft and fraud (including credit card fraud); divulgence of sensitive information, and (b) to Society the systematic recording of citizens' transactions in both public and private databases. Linked databases increase risks (e.g. mistaken identity, inaccurate or out of date information, judgmental profiling).

Must have a detailed agreement by the individual with respect to how their data will be used since without this there is the risk of legal challenge and reputational loss for the organisaiton that collected the data. For the individual, their data may be used in a way that they do not consider appropriate.

Lack of trust in the ability of public sector to handle data securely and protect the individual is also an issue. What can the citizen do who discovers that data held on him is wrong or inconsistent? - perhaps there should be an obligation on the authority concerned to put it right upon notification, and alert other authorities with whom the data has been shared. With increased data sharing, things will occasionally go wrong; this needs to be recognised and the risk mitigated by swift remedy where possible.

Question 4.
Comments: The scope of public authority service delivery and the legal and administrative conditions that have to be met in order to securely share personal data should be determined by what is necessary to help achieve a stated goal. There are opportunities to provide consistent and efficient services through the sharing of data across the public sector with effective and enforced controls using appropriate electronic methods. These provide greater control and auditablility than hard copy, faxes and sending material through the post. Potential risks would occur where inappropriate controls allow data loss or misuse. Paper records of personal data carries possibly greater risks at the individual level, but not on the scale of digitally-held records.

Question 5.
Comments: An example of where the public authorities hold too much or not enough data would be where lack of data sharing frustrates policy implementation. For example, sharing NINO data could help prevent illegal working and implement anti money laundering provisions. Data duplication due to lack of sharing may lead to the retention of multiple copies of the same or similar documents within and across organisations. This results in time wasted supplying/recording similar information for e.g. benefits claims, and the risk of introducing errors, not to mention user frustration. Data collection is generally restricted to supplying necessary information for the original purpose. There may be cases where records have not been destroyed when no longer required; whether they are held in hardcopy or electronically, whilst there are costs associated with storage, there is a cost to manage their disposal or deletion.

Question 6.
Comments:

Question 7.
Comments: Responses from some local authorities to EURIM questioning indicate that the DPA is perceived to be a barrier even when it is recognised in reality not to be; others clearly believe that the DPA is in reality a barrier, citing the Childrens Act as one example where the law is contradictory. Clarity and advice from the ICO was also perceived to be lacking by some. Research undertaken by EURIM indicates that the major barriers to information sharing are in normal working practices. It was identified that it is rarely in the interest of people who have accurate information to make that available to others, certainly not in the short term anyway. They do not usually get rewarded on the information they provide. The benefits of information sharing are usually for the person receiving the information. No incentive. Put simply, the cost of information sharing is commonly borne by a department that does not directly benefit from the sharing. Other barriers are practitioners' ignorance as to why we share information, others see the

information created as ownership to themselves and feel possessive of it. In addition some feel that sharing information would not be ethical. Sharing name and address information between two tier authorities would be beneficial to service delivery, but at present there appears to be a legal barrier to doing this.

Question 8.
Comments:

Section 3: The legal framework

Question 9.
Comments: It is a relevant and appropriate piece of legislation, but needs to be updated if we are to provide efficient shared services. Perhaps there needs to be an exemption for sharing of a defined set of data across the public sector so for example if we are notified of a change of address through the Council Tax process, then the relevant Police authority could be notified so they could update e.g. firearm certificate records. Perhaps the biggest single problem with the DPA is that the Act requires the exercise of judgement - there are no hard and fast rules for every occasion. This has led to fear of sharing data (rightly or wrongly), and there are many examples of the DPA being cited, incorrectly in many cases, as a reason for not sharing data - perhaps the most notorious being the Huntly case.

Question 10.
Comments: A problem with the second principle is where sharing is prohibited unless specified; the list of purposes could be extremely long and there seems to be no real protection for organisations sharing data in accordance with the recorded wishes of the data subject.

Question 11.
Comments: A resolution needs to be found to the current situation where conflict exists between demands for privacy and joined-up, citizen-centric services that require organisations to hold relevant personal data.

Question 12.
Comments: Notification of Security Breaches The introduction of a data breach notification requirement would be an important move in the right direction to increase levels of data security and also help raise awareness, and reassurance, amongst citizens of how their personal data is being secured and protected. That is not to say that the current European Data Protection law (Directive 95/46) is not effective or failing to protect individual's data; data protection law protects the lifecycle of data from its collection, processing to its storage. However, current legislation does not address circumstances where data is lost or stolen. A legal gap therefore exists that needs to be closed particularly in light of the increase in incidents of data being lost or stolen occurring. Closing this gap would not only complement the

current Data Protection legislation but also serve to enhance the security of data throughout its complete lifecycle. It is important to note that any breach laws must include public and private sector organisations within scope.

Given the importance of data security and the potential impact of legislation in this area it is important that the move towards data breach notification is one which is carefully considered to ensure that a clearly defined legal framework and appropriate operational procedures are established that are workable and not burdensome on either citizens or industry. For example the definition of an incident that would be considered a "breach" of data and the level of seriousness a breach would have to be to trigger a notification obligation, would need to be considered. These definitions are a vital part of any data breach legal framework and must be clearly defined so that companies clearly understand when a data breach notification requirement would be triggered. The law also will clearly state what sort of information is defined as personal, and would subsequently trigger a breach. As an example, Connecticut law (stat 36a-701b) covers information that includes a data subjects firstname/surname in combination with Social Security number, drivers license, account number/debit/credit card. Defining what information is covered within the UK will equally need to be decided.

Further consideration would also be needed on how a data breach notification might work in practice; fundamentally in the event of a breach what immediate action would an organisation have to take? For example, should notification be given immediately to only those customers whose information is involved in a breach, or every customer? Should companies be required to notify the National Regulatory Authority (NRA) before alerting customers? An issue that should also be considered further is the information that would be required to be shared with citizens about the breach and the possible content, format and medium that should be used when providing notification. The law should also detail what right of action or enforcement is available to data subjects whose information has been compromised. In the United States for example, there are differing penalties dependent upon the US State in question. In California the law allows for a private right to action, whereas in Arkansas for example section 4-110-108 of the Arkansas code states that any violation is punishable by the Attorney General.

In addition any legal requirement that is drafted must include a "safe harbour" provision to ensure that in the event of a data breach, organisations that can demonstrate that data has been protected to an adequate level of security are relieved from liability and possible legal or financial penalties for the breach. While further discussion would be needed on the technical security measures that would be considered adequate for a safe harbour to apply, ranging e.g. from intrusion detection to encryption, this would only be able to be determined when it is clearly understood what level of seriousness an incident would have to be to trigger a notification obligation.

In addition to being a positive tool to enhance consumer confidence it can be argued that the introduction of data breach notification legislation in US States has had a

positive impact on citizens and their understanding of the importance of data security. It can be suggested that data breach notifications have helped to raise citizen's awareness of the risks their data is being open to and therefore enable them to take appropriate action where necessary. This is supported by a 2006 survey on the costs of data breach in the US, which identified examples of customers notified of data breaches subsequently not shopping with the retailers responsible. By being given information citizens become informed and more empowered to make informed decisions and take measures to protect their identities that may be at risks. Such activities may include monitoring financial accounts for discrepancies, not responding to potential phishing emails related to a data breach or simply ensuring personal information is not disclosed unnecessarily. It can be argued that the action of presenting an individual with a data breach notification letter means that individuals become more aware of the situation and by being fully informed are able to take action they see as appropriate to protect their identity or personal information going forward.

It is important to address the needs of vulnerable members of the community who are not able to understand or act appropriately to the situation. For example an aged or incapacitated individual who has someone as an Enduring or Lasting Power of Attroney. A straightforward process is needed to register as the LPA/EPA or equivalent, e.g. via a website that allows a nominated proxy/agent to register in that capacity as well as the principal.

As an example, consider a son holding an EPA for his mother and wanting a utility company to advise when they bill to her. At present, their system could not allow the son to be notified of changes or bills, much less any information breach. This renders notification of the mother of personal data issues meaningless where she is incapable of dealing with the issue.

Recognising the role of a proxy/agent is important to enable someone to act quickly and appropriately in the event of a breach to limit the consequences of breach. Consideration therefore needs to be given to the process around establishing the proxy/agent consent before a breach has occured and not after it. This is especially important where implied consent holds and there has been no explicit registration process.

A general principle might be established to ensure that when a breach is identified, affected parties are notified as quickly as possible to limit the (potential) damage.

Question 13.
Comments: A recent case in the High Court successfully challenged the right of the Chief Constable of Thames Valley Police to disclose data concerning allegations [of sexual misconduct] about an individual. it was reported that "The legislation allows the police almost unfettered discretion on what information may be included in an Enhanced Criminal Record Certificate"… "Unsubstantiated material can be included, even if there is no criminal conviction or charges, and even if there is no evidence that the allegations are true. This approach was intended to ring-fence the vulnerable, but its effect could be devastating for the wrongly accused.

Question 14.
Comments: An issue to be considered under legislation 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). This may best be addressed by proper implementation of best practice compliance with Principle 7 of the Data Protection Act: new legislation to address these issues of data ownership etc. would then be unnecessary.

Question 15.
Comments:

Section 4: Consent and transparency

Question 16.
Comments: Before we can consider the potential impact of giving consent, are we clear as to what consent actually means to both the requestor and those requested? If consent is given for information sharing for e.g. marketing purposes, does consent endure, can it be withdrawn – is it clear whether and when consent is needed? What differences are there between public and private sector services? EURIM had debated the issue of consent in a series of workshops and meetings over the preceding 3 years, and the debate and the issues appear not to have moved on. Relevant papers are attached and also appear on the EURIM website at: http://www.eurim.org.uk/activities/pi/PI_statusreport_Jul04.doc http://www.eurim.org.uk/activities/pi/0407statusreport.pdf http://www.eurim.org.uk/activities/pi/050113JFtalk.pdf http://www.eurim.org.uk/activities/pi/050113JLtalk.pdf http://www.eurim.org.uk/activities/pi/050421pireport.pdf http://www.eurim.org.uk/activities/pi/0411circleoftrust.pdf http://www.eurim.org.uk/resources/status_reports/EURIMStatusReport8_ModGov.pdf http://www.eurim.org.uk/activities/pi/DS_statusreport_Apr05.pdf http://www.eurim.org.uk/activities/medrecs/020619report.pdf http://www.eurim.org.uk/activities/ecrime/071213_pv-issa-presentation.pdf http://www.eurim.org.uk/activities/pi/050113pireport.pdf

Question 17.
Comments: A major question is ‘how genuine is the consent’? Whether the implications of giving consent are understood or not, there is in reality no choice if the individual wants the service on offer (the terms of use are usually printed in small font, couched in legalese, and overly long, all it seems designed to deter the reader from a full understanding of what they are agreeing to). However, there must be a responsibility by the individual to acknowledge and understand what it is they are signing up to. If a service requires the consent of an individual, then that individual should be able to view

who has accessed their data, and understands to what and to whom their consent is given. This implies that consent involves clear boundaries beyond which their personal data will not be given. Many current examples of terms of use are difficult to understand, raise competency issues and may involve the transfer to the individual of unacceptable costs and liability: it is too difficult in many cases for the individual to judge the impact of their giving consent.

Terms of Use are invariably written for the benefit of the service provider, and the ability of the individual to challenge them is very limited. There is a need for legal guidance as to whether the 'small print' is legally valid, and a practical solution might be to engage a qualified 'champion' to act on behalf of the citizen in the establishment of the Terms and Conditions of Use. Should the ICO have a role here?

Question 18.

Comments: The issue of consent should be considered in the light of current thinking about the different approaches to identity and the management of personal information.

In the traditional, or organisation-centric, approach to these issues, organisations try to link records held in different databases by comparing common fields, typically name, address, and date-of-birth. A cross-organisation unique identifier – such as the NHS number, the Unique Learner Number, or the proposed National Identity number – can make this linkage of records easier and more accurate. Since the process takes place between organisations' back-offices, it need not necessarily involve the individual, or any form of consent process, at all. Criminal records are a case in point. In other cases, the individual is asked - at the time of application to a service provider - for 'broad-brush' consent for whatever information sharing may be required.

An example of good practice here is offered by the financial services industry. Should an individual wish to open a new account with a financial services provider, he or she will be asked to give consent for data-sharing - which will take places via the back-office route, using a credit reference agencies as an intermediary. Concerned individuals can gain access to both a statement regarding the implications of giving consent, and also the name of the specific credit reference agency to be used. Further, and although there is no direct interaction between the credit reference agency and the individual at the point consent is given, the agency will provide a copy of an individual's data in return for a nominal fee, and within a few days of a request being made. This data includes a log that describes who has accessed their data, when and why.

The arrival of the internet now offers an alternative to organisation-centric data sharing. Individuals can be empowered to give direct and explicit permission for the use of their own data, rather than inspecting access logs in retrospect. Note the terminology here: we use the word 'permission', in lieu of 'consent', to imply that the individual is 'in the loop', and has fine-grained, active, and transaction-

specific control over the sharing of her data. Other terms, such as 'user-centric', or 'citizen-mediated', or 'front-office' data-sharing also have some currency, and all indicate the objective of empowering the individual to act as gate-keeper for the use of his own data, so enhancing privacy and enabling many new applications.

In one sense, permissioned data sharing is nothing new. Although negative information – such as criminal records – must always be shared directly between organisations, individuals have long managed certain kinds of personal information themselves, using tamper-proof paper certificates. Examples include medical prescriptions, driving licences, and exam certificates. Generally, such information is positive, or can at least be used for transactions that deliver a net benefit for the individual.

Replicating the permissioned approach electronically requires an emerging technology, one referred to by the (unfortunately clunky) name of 'user-centric identity management'. We again make reference to the forthcoming ICO paper entitled 'New approaches to Identity Management and Privacy'. As stated earlier, efforts are now underway to organise a large-scale pilot of user-centric IdM in the UK, starting in the education sector. These efforts could be accelerated if Government were to recognise the need for such a pilot and provide a fair-wind.

Is there a case for legislators to be required to define the impact of any change in the law in terms of access to information and information sharing, what is mandated, what is prohibited, and the boundaries beyond which sharing will not be legally permitted? In other words to make explicit what is currently left to interpretation?

Should there be a single point of consent with multiple applications, or should each data controller be required to seek consent separately - if the latter, the process would become unmanageable. It would be much better to require clarity on why consent is needed and what it is for, perhaps tested by a trusted third party for plain English.

Question 19.

Comments: Consent should not become an overriding issue especially when dealing with Government, where it is often not required. Transparency is a much more important issue, enabling people to understand what is involved, the implications and the boundaries. Belgium and Slovenia are leading the way in enabling real-time online access for individuals to monitor what information is being shared about them in both public and private sectors, and would be relatively inexpensive to introduce into the UK where it could form best practice.

There is a question about whether a person or organisation holding and/or sharing personal data on individuals should be considered as an agent acting on behalf of those

individuals, with the responsibilities and liabilities of an agent, as opposed to e.g. the civil service claiming Crown immunity for data breaches. The issues of care and responsibility for securing the data retained are currently unclear, with little in the way of advice or guidance. Unless retained data is managed, which is expensive and a potential vulnerability, it rapidly becomes degraded. Protection of data through encryption is an appealing option, but apparently not common practice in Government, where data is frequently 'mislaid', and at times on a massive scale – as shown by recent losses at HMRC, DWP, DVLA and the MoD. Accountability and restitution, with meaningful penalties for breaches of security, would appear to be necessary to supply an effective deterrent to malpractice and to encourage good practice.

Section 5: Technology

Question 20.

Comments: While technological advances have facilitated the adoption of data sharing techniques, available mechanisms for the technological protection of the data have all too often not been employed. Information can be shared more rapidly and in ways not possible with paper data.

Making medical data available electronically actually makes it possible for information to be shared. Paper based systems are in fact no more secure: medical records have been observed stored in shopping trolleys in hospital corridors! Much more data can be created and transported electronically, but technology can deliver accountability where paper-based systems cannot. One of the aspects of the DCSF's database on children, ContactPoint, is that the audit trail records every person's access to the records – not possible in a paper-based system. On the other hand, the availability of an audit system does not guarantee its use or misuse.

At present, for a patient in A&E, their name and address would have to be obtained from a medical records wallet and their GP traced and contacted in working hours to identify necessary information. This would then be transported by courier (or taxi) to the hospital – a very cumbersome and slow means of data sharing that does not benefit the patient and which may cause distress and harm through delay. Secure electronic sharing of the right data at the right time at the right place would have a positive impact on patient experience and health outcomes.

Data quality is often time-dependent; in the medical field, the best source for information is often patients themselves, e.g. a rapid blood test at the time will give more reliable information than current digital or paper records, many of questionable relevance and/or accuracy.

Another issue is the large amount of personal data obtainable in electronic format from digital databases, especially where the information is not differentiated. Access levels given to staff, and staff awareness of technological functionality and change, are also important considerations. Technology facilitates ever more

rapid access to large amounts of data and its subsequent use and distribution, giving a new dimension to 'people problems' and the way in which technology is used. Thus whether the available data sharing and protection technology is used, and how it is used, are relevant concerns.

An advantage of paper is that it is harder to replicate: you can probably recognise the original as opposed to a copy, but this is less clear for electronic documents, and has consequences for detection of change, authenticity and what can and cannot be shared.

The identity card scheme implies a single identifier for public sector purposes, and thus the potential to link up partial records held on different databases to form a single overarching record about the individual. In the terminology of the field of identity management, this is an organisation-centric approach to identity and data-sharing.

In the alternative user-centric approach, an individual continues to use a different identifier for each distinct organisation with which he deals, and may then be empowered to give explicit, transaction-based, consent for the sharing of data between two or more organisations. Note that both organisation-centric identity management (IdM) and user-centric IdM are variants of a federated (i.e. one that crosses organisational boundaries) approach to identity management.

User-centric information sharing is the rough equivalent, in the electronic world, of giving a paper certificate – such as a medical prescription or exam certificate – to an individual. The individual can then choose whether or not to show the certificate to a third party, and presumably will do so if required to enable desired transactions.

We make reference here to a paper entitled 'New approaches to identity management and privacy: a guide for the Information Commissioner'. This was commissioned by ICO in late 2007 from John Harrison of Edentity and Pete Bramhall of HP Labs, and is likely to be published early in 2008.

The technology for user-centric information sharing is now well understood, and efforts are underway to organise a large-scale pilot. These efforts will probably only succeed with cooperation from Government – which, to date, has not been forthcoming.

Most of the recent losses of data by government departments or agencies have been one-off, non-transactional requests, involving 'old' technology; in most transactional systems relatively sophisticated technologies are in place to help secure the records which are not in place for ad hoc requests. A wider issue beyond information security is that technology can confer the ability to access and share data person to person without thinking through why, and without regard to its future use. Issues of control and ownership can thus change power relationships, and education and training of staff is important in recognising this

Technical safeguards are just one element of the ISO 27001 security standard, which includes administrative controls, awareness and physical security. Recent Government data losses have not been due to technology failures, but to procedural and/or security awareness failure. The law should mandate safeguards, but this should be only the outcomes, not the means. Attempts to mandate the means are unlikely to succeed, not least because of the inability of legislation to keep pace with or anticipate technological advances.

Question 21.

Comments: The question arises, should there be a separate body to oversee information security, and if so, what powers should it have? However, this may already exist in the form of the CSIA, although their focus is at a strategic level and is not specific to personal data. If a body is required to specifically monitor and police personal data breach notifications, it would seem sensible for additional powers to be given to the ICO.

The issue then becomes one of enforcement; in the USA there is Data Breach Notification law, which requires companies to notify customers when their personal information had been compromised.

In August 2007 the House of Lords Science and Technology Committee brought out a report detailing the results of their inquiry into personal internet security. One of the recommendations of the report was that the government should pass a law requiring organisations to notify all affected parties in the event of a loss of confidential data. On 3 January 2008 the House of Commons Justice Committee also called for new reporting requirements under the Data Protection Act, as well as greater enforcement powers and improved funding for the Information Commissioner's Office.

An alternative approach is to ask "should the relevant professions require good practice of their members, and penalise those who ignore it?" Professional standards may be used by the courts as common law precedent of what would reasonably be expected in common and civil law actions. Thus properly promulgated and accepted professional standards acquire common law legal force which might be preferable to primary and/or secondary legislation.

However, while it seems only reasonable that professional bodies should have a code of conduct that includes reference to the handling of personal data in the course of professional duties, there are so many bodies involved (not after all just IT ones) that this may not be a practical solution. In many areas of work membership of a professional body is not mandated and even where membership exists, there are not many bodies that have the power of say the GMC or Bar Standards Board to discipline its members.

There is a need to consider whether organisations that do not routinely vet (identity, credit status, criminal records etc.) all staff who have direct or indirect (e.g. IT staff or contractors) access to sensitive personal data in the course of their work , are following good data protection practice, whatever their nominal systems" .

Question 22.
Comments:

Section 6: International comparisons

Question 23.
Comments: Several states in the USA have passed data breach notification legislation, but others have not. In June 2007, California's legislature moved a data protection bill that would shift the burden of consumer notification regarding data breaches away from financial institutions and onto retailers. Data thefts were on the rise in the retail sector, with consumers increasingly finding that information stolen at the retail level was bring used to commit identity theft and plastic card fraud. However, in October 2007, California Governor Arnold Schwarzenegger vetoed legislation that would have prohibited businesses from retaining certain payment card data after authorization of a transaction, unless a specified exception applied. Schwarzenegger's veto was based on concerns that the new law would potentially conflict with private sector data security standards such as the Payment Card Industry Data Security Standard and would increase the costs of compliance. There is also an issue of how far UK legislation can apply, where the data controller may be in the UK, but the data is held and administered elsewhere. What are the practical enforcement mechanisms, and where do liabilities, rights and responsibilities lie on an outsource chain? In UK law, the ultimate responsibility is on the data controller, but few sanctions are available as a remedy. Evidence taken for the EURIM Information Sharing Protocols Status Report has revealed from people engaged in public sector information sharing that the UK legal framework is not transparent to the average department or individual. A copy is attached.

Question 24.
Comments: In Belgium, the Crossroads Bank for social security is actually a data bank: a highly-distributed data source with information is held in multiple sources, forming a virtual database to which any of the Belgian institutions involved in social security may have audited access, but only to those data elements for particular individuals for which they have permission, through express authorisation (for more information, see http://www.ksz-bcss.fgov.be/En/CBSS.htm). Identity management involves field level (not just record level) security in a federated system. Advantages include gains in efficiency (lower costs, more services delivered more rapidly with better social and fraud protection; see http://unpan1.un.org/intradoc/groups/public/documents/UN/UNPAN023391.pdf) A very similar system operates in Slovenia.

A counter to the advantages was seen in Estonia in April 2007, when distributed denial-of-service attacks began against Estonian computers, allegedly from Russia, affecting all government institutions and key businesses.

Shibboleth is an initiative to develop an open, standards-based solution to the needs for organizations to exchange information about their users in a secure, and privacy-preserving manner with Web Single SignOn across or within organizational boundaries. It allows sites to make informed authorization decisions for individual access of protected online resources and is developing architectures, policy structures and practical technologies to support inter-institutional sharing of web resources subject to access controls.

Question 25.

Comments: Another example is Megan's Law, which is an informal name for laws in the United States requiring law enforcement authorities to make publicly-held personal information available to requestors regarding registered sex offenders. The basic intention of Megan's Law is to give parents the ability to protect their children by making them aware of the presence of convicted sex offenders in their neighbourhood.

Proponents have correctly pointed out that information about convicted criminals has always been public information, but Megan's Law makes it easier for parents and other concerned individuals to access this information without having to do laborious research. Critics of Megan's Law argue that efforts to establish sex offender registries are based on the widespread misconception that child sexual abuse is commonly committed by strangers, whereas most children are abused by someone they know and trust.

Jessica's Law is the informal name given to a 2005 Florida law, as well as laws in several other states, designed to punish sex offenders and reduce their ability to re-offend. Forty-two states have introduced such legislation since Florida's law was passed. The law is named after Jessica Lunsford, a young Florida girl who was raped and murdered in February 2005 by a previously convicted sex offender. Public outrage over this case spurred Florida officials to introduce this legislation which carries a mandatory minimum sentence of 25 years in prison and lifetime electronic monitoring of adults convicted of lewd or lascivious acts against a victim less than 12 years old.

Question 26.

Comments:

Section 7: Additional questions

Question 27.

Comments: Government should show practical leadership in implementing data sharing within an overall identity management strategy that reduces and simplifies the amount of legislation impacting on data protection and sharing within the public sector, while regaining public trust, in order to help realise citizen-centric and efficient public service delivery.

Question 28.
Comments:

Full name	David Thomas Wright
Job title or capacity in which you are responding to this consultation exercise (e.g. member of the public etc.)	Deputy Secretary General
Date	13 February 2008
Company name/organisation (if applicable):	EURIM
Address	15 Catkin Drive Giltbrook Nottingham
Postcode	NG16 2UB
Address to which the acknowledgement should be sent, if different from above	
We work on the assumption that we will publish the responses we receive. Please state explicitly if you want all or parts of your submission to be treated as confidential, explaining why. Please note, that this does not in itself guarantee confidentiality (see 'Publication of summary of responses' section below).	Submission is not confidential
We intend to hold more in-depth interviews with certain respondents. Please indicate if you would be happy for us to contact you.	Yes, I would be happy to be contacted ☒ No, please do not contact me ☐

Publication of summary of responses

Following the end of the consultation we will publish a paper summarising the responses. The response paper will also be available on-line.

Information provided in response to this consultation, including personal information, may be published or disclosed in accordance with the access to information regimes (these are primarily the Freedom of Information Act 2000 (FOIA), the Data Protection Act 1998 (DPA) and the Environmental Information Regulations 2004). Although information held by the Review Team is not covered by the Freedom of Information Act we intend to operate a voluntary access scheme in keeping with the FOIA, and please be aware that the majority of the Review's information will be handed over to the Ministry of Justice for long-term preservation at the close of the Review, and the Ministry is covered by the FOIA.

If you want the information that you provide to be treated as confidential, please be aware that, under the FOIA, there is a statutory Code of Practice with which public authorities must comply and which deals, amongst other things, with obligations of confidence. In view of this it would be helpful if you could explain to us why you regard the information you have provided as confidential. If we receive a request for disclosure of the information we will take full account of your explanation, but we cannot give an assurance that confidentiality can be maintained in all circumstances. An automatic confidentiality disclaimer generated by your IT system will not, of itself, be regarded as binding on the Ministry.

The Ministry and the Review will process your personal data in accordance with the DPA.