Annex E: Consultation Questions

The consultation sets out a number of proposed amendments. Views are invited on the following:

1) Where data relating to a citizen is held it should be accurate. Do you agree that the approach suggested in paragraphs 9-11 is an effective approach to achieving this?

Yes ☐ No ☑

If No, please describe the approach you feel should be taken.

No.

For data relating to a citizen, or citizens, person centric approaches are significantly more trusted than organisation centric ones. Organisation centric approaches are more costly, more prone to error and large databases are very risky and susceptible to attack or failure.

Person centric approaches tackle inequality, promote equal participation and collaboration, grow the economy and significantly increase engagement, inclusion and trust.

These values are what underpins a fair society and co-design, trust and self management are preferable for citizens to feel valued and included in their interactions with services.

An approach as suggested is a possible approach, but an organisation-centric approach to data sharing will always be less accurate compared to one that is built on trust and includes the citizens of Scotland in participation and inclusion.

The approach in paragraphs 9-11 is not effective as it does not include citizens, and trust is not established with the participation of the people of Scotland.

It contradicts the Scottish Government’s Identity and Privacy Principles


The Scottish Government and public sector could empower citizens by re-using data attributes such as those in the “myaccount” and enabling the verified attributes to be passed to the citizen.

These personal data properties of the citizens of Scotland should be given to citizens, thereby enabling them to be passed to a Scottish citizen’s Personal Data Store (PDS).

The approach where individual citizens are also included will be more accurate and there will little time delay in achieving this accuracy. If citizens can see that
there is a benefit in volunteering data, then there is a basis for mutual collaboration, a more trusted "social contract" and a Scottish trust framework.

Where organisations try to share data without the citizen being aware, then there is not consent, trust, accuracy or a sense of shared responsibility. There is also not the explicit consent of the citizen so it may contravene EU Laws in relation to privacy and other substantive issues.

The Scottish Executive published in 2010 a Paper specifically stating that sharing Persistent Identifiers are not the right way to go. The Chair of the Identity and Privacy Principles was the Head of the Data Management Board and is now the Head of the NHS in Scotland and these Principles in 2010 are equally true and relevant in 2015. The Chair of the Data Management Board should have been asked to review this proposal as it directly contradicts many of the Privacy Principles that were agreed in 2010 and amended slightly in October 2014.

There is also no Privacy Impact Assessment attached to this Consultation to build a Scottish National Identity Database. As such the Consultation is incomplete and cannot be reasonably interpreted or understood.

The Information Commissioner is also not listed as part of the PIA process, and should be consulted for an Opinion on the Scottish National Identity Database that is proposed to be created by this Consultation.

Identity Management and Privacy Principles (revised in October 2014)

What happens if individuals can control their personal data and work with the system?

More benefits of connecting to individuals' "Personal" Data Stores

Apart from the legal clarity and empowerment of individuals, taking the approach of connecting Scottish Government and other public sector systems to individual "Personal" Data Stores has considerable other benefits:

- It’s a basis for more trusted digital services.
- People who control their own data can easily and instinctively identify errors and provide corrections back to service providers. They can fill in gaps and update outdated information and reduce errors.
- Making “verified public sector data” available to the citizen – such as proof of address, proof they are on a form of benefit or another, confirmation they have had a face-to-face meeting with Scottish public sector organisation and that their passport, driving licence or other forms of physical evidence have been inspected to a recognised standard by trained personnel – helps people in turn get other things done online (from ID assurance to claiming cheapest tariff from an energy supplier).
- A “digital letterbox” capability sitting between Scottish public sector organisations and the individual eliminates the very considerable costs of printing, fulfilment and postage. Digital delivery is shown to increase response rates, and Scottish public sector organisations would then have evidence of receipt for every communication.
- Omni channel support: increasingly citizens engage with public sector and other organisations across multiple channels: face to face, telephone, websites and mobile device based apps. But all too often these channels are not integrated at the back end. With a "Personal" Data Store in place, connected to each channel’s underlying systems, the citizen and organisation can ensure all information is there just when it is needed. This means new customer journeys can be created that cross channels seamlessly. This supports Scottish and UK public sector channel shift and lets Scottish and UK public sector organisations assign channels more easily, with increased customer satisfaction.
- Putting individuals in the loop offers a realistic basis for genuinely personalised services in a way that connecting the institutions simply cannot match.

Other benefits

The current modes of sharing seem to be limited to Organisation to Organisation, and take no account of citizens or democracy.

Elsewhere in this context, there is no Consultation on where the Scottish Government is creating additional, other new Databases in Scotland and how they relate to this Organisation Centric Scottish Identity Database.

The Information Services Division within the NHS is looking to create a system which allows assessment of health and social care data at an individual level, with the purpose of supporting effective commissioning. From what I understand however, individuals are not involved in this process. More information is available via this link:

http://www.isdscotland.org/Health-Topics/Health-and-Social-Community-Care/Health-and-Social-Care-Integration/

In Scotland, our institutions have traditionally made changes by consulting openly and transparently, and by pointing out the implications of the proposed changes. This is with the widest possible range people, with civic society and with Parliament in the widest possible way, with openness and with transparency. Our citizens have been able to enter into a dialogue about issues.

Other jurisdictions that Scottish politicians admire e.g. Scandinavia do not practise data sharing without any regard to the individual. The Dane, Swede or Norwegian individual citizens trust their service providers as they have been able to have a more open and transparent dialogue. This builds a trust framework between the participants, and can happen in Scotland.

Scotland’s current Organisation centric data sharing practices contain barely a cursory notion of consent of the citizen. We believe that much further work needs to be done in the Parliament, across civic society, across the public sector and
with the people of Scotland to understand the value and potential of genuinely citizen centric enabled data sharing. This goes beyond the notion of an "in transaction consent process ", to the much more trusted provision of verified attributes, proofs of claim and data being shared directly with the citizen to be held in their own personal data store. A "personal proof bank" if you will. The data itself will be secured cryptographically so that relying parties can trust it. Trust that it was issued by a specific issuing authority. Trust in the process of issuance. Trust that it has not been modified in transmission or storage since issuance.

This approach opens up the potential for Government to act as a verified attribute provider. For the citizen to be an active participant and for the notion of collect once and share many. It removes the complexity of providing API access between government systems, and downstream third and private sector access to government systems. It extends the notion of a citizen’s personal data account or personal tax account into something genuinely personal under their control and removes the issue of loss of contact. A personal data store with secure, encrypted and persistent connection to a citizen’s records across government mean that once verified, subsequent and connected transactions can be seamless.

This empowers citizens, and enables the person to be at the centre of health & care integration; criminal justice; education; self-directed support; self management. Citizens can work with public services.

We ask the Scottish Government Consultation to take on board the citizen centric approach.

The Scottish Government Identity Management and Privacy Principles accept Person Centric approaches to Identity Assurance, and state at Paragraph 4.5

Storing identifying information

4.5 Public service organisations must consider whether identifying information needs to be stored in a database at all. In some cases, it might be preferable for people to hold and manage their own identifying information which can be accessed by the public service organisation when it is needed


It would be very regrettable if all Scottish citizens had their data shared with the Scottish Meat Quality Commission, and 200 other bodies and 100,000 medical researchers but none of their data was ever shared, controlled and curated with and by the Scottish citizen themselves.

If citizens have personal control over personal data, this creates a halo of trust around the individual, their connections with service providers reach out across all aspects of their life and it cuts out paper and manual based processes, reduces the risk of fraud and error and cuts out the repetitive nature of form
filling. An individual equipped with their verified data and proofs of claim can become empowered and enabled to move to digital by design / default by preference.

This can deliver cost savings in public services, streamline customer journeys and improve satisfaction. The current approaches being discussed are grouped under the concept of organisation to organisation data sharing often described as the "Crown of Thorns" approach as the citizen is excluded, remains an unequal participant, remains isolated, lacking in control and transparency and the entire approach is costly, transaction centric and prone to poor data quality and risk of abuse.

Please see recent white papers on the concept of attribute exchange

https://mydex.org/blog/2015/02/03/mydex-cic-white-paper-opportunity-attribute-exchange/
http://www.theinformationdaily.com/

Video

http://www.theinformationdaily.com/2015/02/17/answertime2-highlights

Articles on Crown of thorns approach to data sharing

https://mydex.org/blog/2014/08/28/crown-thorns-stifling-innovation-online-services/

Halo of Trust – person centric data sharing

https://mydex.org/blog/2014/10/10/halo-trust-unlocks-potential-digital-services/

Policy Exchange paper on data sharing

https://mydex.org/blog/2015/02/03/policy-exchange-publish-paper-data-local-government/

Contribution to DWP consultation on data sharing


Nine ways personal data can transform public services

https://mydex.org/blog/2014/12/23/nine-ways-personal-data-store-can-transform-
2) We propose to extend the current ability to trace persons a) who go missing whilst in education and b) who should pay for treatment provided by the NHS. Do you agree with these proposal set out in paragraphs 12-13?

Yes ☐ No ☑

If No please explain why not?

Volunteering personal information is a decision for the individual. There are existing ways to enable these services and to find people.

If a person goes missing, sharing their personal data is not necessarily an appropriate way to trace them. A person may have other verified data attributes that they may be willing to share in advance of the treatment, and it will always be more empowering for the citizen if they are involved in assisting the public sector.

In the health sector, there are ways of establishing who people are, and in other jurisdictions different methods have been designed. In the EU there is a cross border process that already provides citizens with E111 cards for health purposes, and this process enables tracing.

Canada and other jurisdictions should also be considered for their models to deal with different tiers of Government. People in Canada may move between different tiers of Government and have a person-centric identity service to do this.

Essentially the individual does not change. They are the key.

Service providers change all the time and must be person-centred to understand the whole system, and empower the individual.

3) In order to allow citizens to make use myaccount for a wider group of services (beyond health and local government), as set out in paragraphs 14-16, we propose to provide access to the bodies named in draft Schedule 3 (Annex B). Are there any additional service providers who you feel should be included?
"myaccount" is a collection of data attributes and a citizen of Scotland should be the first person and legal entity to hold those attributes.

"myaccount" is not mine as it is held behind a firewall by the public sector. The possessive pronoun is not appropriately used in this sense.

An individual may live in my flat, and has the key to enter it.

But the individual at present has no means to obtain my data from "myaccount", or my health record from the GP. People cannot learn about themselves, nor can they work with public services in the scenario proposed in the Consultation.

The "myaccount" is currently completely the property of the Scottish State, and is in no way at all "mine" in the normal sense of the word.

Only the individual should give consent for anyone else, or any other "bodies" to see the "myaccount" data. Then there will be trust in the system.

What MSP would wish their UCRN to be known by Police, HMRC, Schools, Local Authorities, Mental Health Services, all Doctors, Medical Researchers and Clinics and the other 200 bodies in the list?

Any attempt by any public sector body, or staff to access this data should be prevented. Recent events with newspapers, and public servants illegally obtaining personal data have shown how dangerous it is for data to be made available to anyone without regard to the consequences.

This is a honey pot for crime and attack by cyber criminals.

The data attributes belong to the citizen, and a person-centred Scotland would empower citizens to obtain and curate their personal data in a collaborative way with organisations.

No additional service providers should access the data. Only the individual should be able to share personal data.

The first named legal entity in the left hand columns of Schedule 2 and Schedule 3 must therefore be the Individual citizen.

The individual citizen can then give authority to the local government, health providers and other public sector service providers if they wish to do that, and share personal data based on personal choice and control. All personal data can flow through the individual. This is a basis for trust, effectiveness creating benefits for all concerned.

In Schedule 2, Column 2 - the first legal entity to whom the data should be given is the citizen. The citizen can then have personal control over their personal data. Organisation to organisation data sharing risks disempowering citizens, risks a database state that is vulnerable to attack.
It would be a more appropriate vision and understanding for democracy in Scotland to have consideration for the role of Scotland’s 5.3 million people in self management of personal data. The individual should have personal control of personal data.

In Schedule 3 - the first entry should be “All citizens of Scotland” as citizens are the legal entity to whom the data belongs, and Scotland’s people can then decide with whom to share. This is proportionate, inclusive and empowers citizens and tackles inequality.

This establishes trust, data accuracy and the basis for collaborative and effective working. The citizen has one identity that they own, and they will know when they move address, or change an attribute and they can control this and can tell organisations. Organisations do not need to have a separate database for the same person, as this is more costly, inefficient, open to error and mismanagement.

By only sharing data between organisations, the State perpetuates inequalities among Scotland as the individual citizen has no role, and it does not create responsible citizens able to engage and participate in services.

This Organisation centric approach to data sharing, the sharing of data about individuals directly between institutions, presents a growing range of legal and logistical problems. There are real issues of information logistics, of cost and data quality, of consent, permission and regulatory compliance. It’s also fundamentally dis-empowering for individuals, who have long since lost any sense of clarity or control about what happens to their personal data - who it is shared with and on what grounds.

Proposing these new regulations does little to address the core of these problems, and does nothing to change the realities of European law. It doesn’t make the organisation-centric model any more efficient, doesn’t clean up the data and doesn’t empower individuals.

On the other hand the straightforward introduction of a person-centric model holds great promise. It’s technically elegant, inexpensive, has rapid business benefits and is legally robust. It does not require new regulations.
The Scottish Government is in an influential position to empower Scottish citizens, and to benefit hugely itself, from starting to implement a more person-centric approach to data sharing. Putting individuals in control of the data sharing process, instead of always having organisations share ever more data about them with each other, offers significant cost, efficiency and regulatory advantages. It reduces risks related to data sharing. It will also help individuals acquire and prove trust, learn about, understand and take a much more active part in the digital economy. By enabling them to have control of their own verified data they can access services online more easily.

In a Scotland where the person is at the centre, the first legal entity on the list in Schedule 3 is, therefore, the individual citizen. A citizen has a right to control their personal information and to know what is happening to it, or stop it being shared without their consent or knowledge. Scotland can show much more ethical and moral leadership here, and empower all citizens with our data attributes.

It does not seem appropriate to have the long list of individuals and organisations who can obtain data about Scottish citizens. This increases risks. A medical researcher, for example, across the world does not need all the UCRN data of the Scottish public. This is open to potential abuse, crime, insurance consequences, selling of data and tracking and linking of citizens’ data without their knowledge or consent.

The Scottish Government and others in the UK are already releasing sensitive data to other countries such as the USA and Scottish citizens have not had the opportunity to join the debate, or to give their consent. This is not in accordance with consent, or explicit volunteering of the data. Scotland’s Parliament may not wish this to continue.

Before moving personal data to other countries, the Scottish Parliament and Holyrood legislature must have an open, honest and transparent debate based on open dialogue and primary, transparent legislation.

Otherwise Scottish data will continue to be lost-


By sharing sensitive, personal data across the NHS and any other of the 200 many bodies listed and the many other individuals, the risk of there being data leakage to inappropriate criminals or inappropriate use by journalists, businesses, public servants and others increases exponentially.

The Privacy Principles of the Scottish Government in 2010 highlighted the risks of large databases. These risks are being increased by this Consultation as it creates a Scottish National Identity Database.
There is no such thing as anonymous data and all Scottish citizens are at risk and will be traceable back to the data.

4) Do you consider that the proposals set out in paragraph 18 are an effective method to identify Scottish Tax payers?
Yes □ No x□

If No please describe the approach you feel should be taken.

No.

There should be a Consultation with the Westminster and the Holyrood Parliaments to obtain a much more in depth and proportionate understanding of the cross border issues. The Smith Commission and the EU cross border Directives mean that citizens have processes to engage with that protect their privacy, while ensuring tax is collected.

Tax payers resident in Scotland are already on the HMRC database and have a UTR. A tax payer can volunteer additional personal data in order to establish and inform their tax residency and other requirements.

The Scottish citizen is responsible for this, and can be empowered to do this.

This UTR is an example of a verified data attribute that the citizen in Scotland can use now, and in the future. The UTR is a data attribute that belongs to the citizen of Scotland and it should be under their control where it is used.

This attempt to change methods should be the subject of primary legislation in Scotland and in UK Parliaments to have an open and transparent debate.