Scottish Government response to data sharing code of practice consultation

1. We intend to revise the code to address the impact of changes in data protection legislation, where these changes are relevant to data sharing. What changes to the data protection legislation do you think we should focus on when updating the code?

- What documentation is required, when it is required (or when it is not) and what should be included/recorded
- It would be worth making mention of the Digital Economy Act as a means to share data for public bodies.
- More information on privacy notices, what they should include (I.e. should links to other organisation PP be included?), and that they should be written in a manner which makes them accessible
- The code should address the complexities of supply chains: it can prove challenging in modern digital services to understand where responsibility lies, and can also prove challenging for an individual/data subject to understand how the organisation works
- Can the code please address whether it is appropriate to use consent as a legal basis for bulk data shares in the public sector?
- The Code is very focussed on data sharing between two organisations that are Data Controllers. The Code could provide more guidance in relation to Data Controller to Data Processor arrangements, particularly where there is a contractual relationship.
- Explicitly state that the GDPR turns what was considered good security practice from DPA1998 into a legal minimum, as this is still very much misunderstood

2. Apart from recent changes to data protection legislation, are there other developments that are having an impact on your organisation's data sharing practice that you would like us to address in the updated code?

☒Yes

☐No

3. If yes, please specify:

- The key development impacting this area is the speed of change; digital service delivery done properly embraces change and as such our code should also help organisations embrace change. The code should provide guidance/examples on how to deal with change as a normal part of operation, not as an exception.
- The code could provide more guidance in relation to Data Controllers sharing information with a contractor who will be responsible for processing the data but is also a Data Controller e.g. Solicitors and Consultants.
- Assuming this includes the new GDPR considerations, then will the new guidance pick up on the key new elements of data protection legislation which will have a bearing including in a contract scenario such as; the individual right to erasure of information by a data subject and the handling of that, new rules around consent particularly as affirmative action can be

needed and types of proof needed, guidance around notification of breaches - where this is required and when.

- Some guidance about the new broader definition which now includes online location data, genetic data and online identifiers.
- Worth the guidance making some links with cyber security issues (albeit Scottish Government cyber security colleagues may need to be asked about this or have already highlighted this. They should be asked in any event if they are comfortable with this point) where personal data is being shared.

4. Does the 2011 data sharing code of practice strike the right balance between recognising the benefits of sharing personal data and the need to protect it?

☒Yes

☐No

5. If yes in what ways does it achieve this?

- Using examples/case studies to demonstrate how balancing the benefits of sharing and protecting the data can be achieved.
- It strikes the balance between sharing and privacy; however more extensive, clear examples regarding supply chain and complex ecosystem service delivery (as noted above) should be addressed

6. If no, in what ways does it fail to strike the right balance?

N/A

7. What types of data sharing (e.g. systematic, routine sharing or exceptional, ad hoc requests) are covered in too much detail in the 2011 code?

N/A

8: What types of data sharing (e.g. systematic, routine sharing or exceptional, ad hoc requests) are not covered in enough detail in the 2011 code?

- Sharing data between different parts of the organisation
- Sharing data in response to Enforcement purposes
- It would be useful if the code differentiated more clearly between controller to controller data sharing, and transfer of data to be processed by an external data processor, we struggle to explain this to our staff due to the use of the same terminology for processes that have very different legal implications and requirements
- The focus of the 2011 guidance is primarily around sharing between organisations. It does briefly cover sharing information internally between different parts of the same organisation at **page 10.** The main guidance there though is that that much of the guidance is also relevant in that scenario.
- It may be helpful to have case studies/examples specifically covering scenarios where information may be shared by different parts of the same organisation.

- Those case studies could perhaps help to make clear the types of information and those situations where this can be permissible. These could make clear situations perhaps where common law powers apply, where processing for exercising statutory, governmental or other functions apply, for legitimate interests, or which clarify what is reasonable to be shared internally and that people would be likely to expect and not reasonably object to if given the chance.
- Some more general case studies may also be helpful.

9: Is the 2011 code relevant to the types of data sharing your organisation is involved in? If not, which additional areas should we cover?

- There is nothing detailing the stats and research exemptions when it comes to individuals rights. There are a number of exemptions around this area that should be mentioned.
- Sharing data between different parts of the same organisation
- Sharing data in response to Enforcement purposes

10: Please provide details of any case studies or data sharing scenarios that you would like to see included in the updated code?

- Any case studies around Big Data sharing would be helpful
- Also case studies on shared services, particularly those that form part of UK government eco-system
- Case study on how to implement appropriate technical and organisational measures to ensure and demonstrate that processing of personal data is performed in accordance with the GDPR
- Case study on restricted transfers of data outside the EU (including information on third and fourth party assurance activities and security considerations).
- Guidance of information security contractual T&Cs should be included in contracts with data processors. Example information security contract clauses would be welcomed.

11: Is there anything the 2011 code does not cover that you think it should?

- Would like to see within mergers and takeovers section some guidance on these activities by non-EEA businesses, and how the code suggests approaching these. In the fast paced, digital world, particularly Cloud, this is a constant risk.
- Make it clear that organisations should focus on security outcomes, and not treat security as a compliance exercise.
- Not mandate a single approach – there is a multitude of good practice and guidance material available that organisations could follow; they should use the one which is most appropriate and measured in their situation.

12: In what other ways do you think the 2011 code could be improved?

- A template with clear guidance covering best practice Data Sharing Agreements would be helpful
    - Section 7 could benefit from more detailed cross referencing to NCSC best practice, Cyber Essentials, 10 Steps to Cyber etc.
    - Page 42 refers to a model consent form, a template would be of value here, aligned to the code, showing best practice
    - Page 43 refers to a diagram showing how to decide to share data, an example diagram would be of value here