WALES AUDIT OFFICE
SWYDDFA ARCHWILIO CYMRU

Wales Audit Office / Swyddfa Archwilio Cymru

24 Cathedral Road / 24 Heol y Gadeirlan
Cardiff / Caerdydd
CF11 9LJ
Tel / Ffôn: 029 2032 0500
Fax / Ffacs: 029 2032 0600
Textphone / Ffôn testun: 029 2032 0660
info@audit.wales / post@archwilio.cymru
www.audit.wales / www.archwilio.cymru

Elizabeth Denham, CBE
Information Commissioner
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Sent by email: datasharingcode@ico.org.uk
Date issued: 06 September 2019

Dear Ms Denham

Data Sharing Code Consultation

We are grateful for the opportunity to respond to your consultation on the draft updated data sharing code of practice. I am responding on behalf of both the Auditor General and the Wales Audit Office.

The code clearly has relevance to data sharing by the Auditor General in terms of his own processing. It may also usefully inform his work at audited bodies, for example, under the Well-being of Future Generations (Wales) Act 2015. Under that Act he has a responsibility to examine the extent to which the bodies are acting in accordance with the Sustainable Development principle in setting and pursuing Well-being Objectives, which includes their need to take account of the benefits of collaboration (one the "five ways of working"). The Data Sharing Code may therefore be a useful tool for auditors in considering whether audited bodies are acting in both a sustainable and legal way.

Q1 Does the updated code adequately explain and advise on the new aspects of data protection legislation which are relevant to data sharing?

Overall, we think that the Code adequately explains and advises on key aspects of data protection legislation which are relevant to data sharing. We think that the explanations about accountability could be clearer, as outlined under Q2.

Q2 if not, please specify where improvements could be made.

We think that the chapter on **accountability** could provide a clearer explanation of the types of records that should be maintained to demonstrate compliance with the GDPR, and so meet the accountability principle.

The section on ‘What documentation do we need to keep?’ states that ‘You must document together all aspects of the data sharing, and other aspects of your compliance with the data protection legislation, such as your record of the lawful basis for processing and the privacy information you provide’. We think this is unclear and could be interpreted to mean specific records of data sharing activity or more widely to documentation recording all personal data processing, such as a data mapping record. Clarification of whether data controllers should maintain a central record of all its processing or whether records can be kept locally would be helpful.

The colloquial terminology ‘hard wiring’ could be misinterpreted and it might be clearer to state that data protection by design should be embedded into an organisation’s practices.

We think that the examples provided are helpful, though could provide further detail as to how to demonstrate good practice in meeting the accountability principle.

Example 1 appears to suggest that a DPIA would be useful. An improvement to this section would be to expand on whether a DPIA both achieves and demonstrates compliance.

Example 2 (NHS protocols) as above, it would be helpful to clarify if the situation in this scenario is enough to demonstrate that the accountability principle was met.

Q3 Does the draft code cover the right issues about data sharing?

Overall, we think that the Code covers the right issues. We think that further explanation about data sharing required by statute would be helpful, as outlined under Q4.

Q4 If no, what other issues would you like to be covered in it?

We suggest that the Code explains that concerns regarding data sharing should not be used to impede the provision of information in accordance with statutory obligations. We think it would be helpful if the code recognised that obstruction of legal obligations to share information may be a criminal offence.

Q5 Does the draft code contain the right level of detail?

Yes, and the links to further ICO guidance, other resources and the legislation are helpful.

Q6 If no, in what areas should there be more detail within the draft code?

Not applicable.

Q7 Has the draft code sufficiently addressed new areas or developments in data protection that are having an impact on your organisation’s data sharing practices?

Yes

Q8 If no, please specify what areas are not being addressed, or not being addressed in enough detail.

Not applicable

Q9 Does the draft code provide enough clarity on good practice in data sharing?

We think that where examples are provided these are largely useful, though in some cases further clarification would be useful, as explained in the answer to Q2.

Q10 If no, please indicate the section(s) of the draft code which could be improved, and what can be done to make the section(s) clearer.

There are some chapters where there are no, or limited examples of good practice and these may be beneficial in the following areas:

1. lawful basis,
2. fairness, where it might be helpful to have a scenario which demonstrates where sharing negatively affects someone but is not unfair. Similarly, an example to illustrate the privacy information that would be relevant in different situations, eg, routine sharing versus ad hoc requests,
3. security, where an updated version of the sample questions in the 2011 Code on physical and technical security would be helpful, rather than broad statements about developing 'a culture of compliance and good practice',
4. data sharing and children, where examples of when a child's data may be shared, and how to do this lawfully and in the best interests of the child would be helpful. When following the further reading link there are no examples and a circular link back to the Data Sharing Code, and
5. data sharing and emergency situations – a checklist would be helpful to support staff to make logical decisions when under pressure.

Q11 Does the draft code strike the right balance between recognising the benefits of sharing data and the need to protect it?

Yes, we think the code provides a reasonable balance.

Q12 If no, in what way does the draft code fail to strike this balance?

Not applicable.

Q13 Does the draft code cover case studies or data sharing scenarios relevant to your organisation?

Yes. There is a relevant case study about an anti-fraud exercise and data sharing required by law (page 103). We suggest that the case study recognises that authorities should not use specious data protection concerns to obstruct legally required sharing of information.

Q14 Please provide any further comments or suggestions you may have about the draft code?

We think that the updated draft Code explains and advises at a high level on the key aspects of data protection legislation which are relevant to data sharing, and refers the reader to appropriate ICO guidance, or other resources, on specific topics.

However, we have some suggestions for improvement:

- Organising the order of the Code to follow the chronology of data sharing in practice,
- Reducing replication of information, where similar information is found in the summary, the 'at a glance' section and the main body of the topic,
- Using a consistent style of writing throughout the Code, so new sections and sections that have been retained or extracted from the 2011 code are in harmony,
- Using language and terminology that is accessible and unambiguous, to avoid possible misinterpretation, perhaps reducing the use of figures of speech, for example, 'hard wired', 'put off', 'along with' (in the context of joint controllers), 'the essence of the agreement' (in the context of providing key privacy information about a data sharing agreement), 'state of the art', 'make life easier for yourself..', 'lawful in a more general sense', 'bear in mind'.

We think that information in some areas of the draft code could be presented more effectively for the code to support data sharing that is not only responsible, but also compliant, and our observations are outlined below.

About this Code

The 'About this Code' chapter has separate sections on the status of the code and its purpose, with some duplication of content which could be reduced by arranging the sections together.

The section on who should use the Code says that it is 'mainly for' controllers but does not explain any other uses of the code, such as whether it may be relevant within a large organisation with a wide range of functions. The section also contains information about the use of the code rather than who it is for.

Some of the wording is grammatically unclear and potentially confusing, for example, the indication that if you don't comply with the code it will be more difficult to show that your data sharing is accountable. Data protection law requires that controllers comply with the accountability principle, rather than the sharing itself being accountable.

The 5 boxes seeking to address misconceptions extend the length of the Code, with some restating information which is set out elsewhere in the section or later Chapters of the Code (eg, the benefits of sharing).

The Code provides three examples illustrating the benefits of data sharing, all of which relate to health (and therefore special category information). It would be helpful for the examples to be more widely drawn to demonstrate the benefits across different sectors.

Data sharing covered by this code

The chapter on ‘Data sharing covered by this Code’ states that the code does not cover data sharing with employees or processors – it would be useful to direct the reader to where guidance on how to share such data lawfully may be found

The section on ad hoc or one-off data sharing is very brief. The Code refers to planning for contingencies and this could be expanded to explain the types of things organisations could do as part of their planning and give examples of situations where these requests may arise. The 2011 Code advises on having ‘established rules and procedures’ for such situations and further advice might be helpful, particularly in light of the accountability principle.

Deciding to share data

We note that there appears to be an absence of reference to the lawful basis for sharing, before exploration of deciding whether to process data. The focus of this section appears to be on the purpose of the sharing, its benefits and what the sharing is seeking to achieve.

The lack of information about the lawful basis for processing early in the Code could lead to controllers deciding to share without first establishing the lawful basis. There is no reference to the additional basis for processing special category or sensitive personal data until the lawful basis chapter of the Code, which appears less than helpfully later in the draft Code.

The questions provided appear to be framed around planned sharing and do not provide clear guidance on ad hoc or one-off requests.

Data Sharing Agreements

The paragraph on legal indemnity is ambiguous and plainer English could be utilised to explain the principle, (which appears to be that a data sharing agreement is not evidence of legal compliance, the ICO can still take enforcement action, but an agreement will however be considered in an ICO investigation).

Other legal requirements

We think that the language referring to data sharing being ‘lawful in a more general sense’ is unclear. We would recommend keeping the useful section on data sharing from the 2011 Code.

I hope that this response is helpful. I should be happy to discuss any of the above matters.

Yours sincerely

[redacted]