

ICO call for views on updating the data sharing code of practice



Data sharing can bring important benefits to organisations, citizens and consumers, making our lives easier and helping to deliver efficient services. It is important, however, that organisations who share personal data have high data protection standards, sharing data in ways that are fair, transparent and accountable. We also want controllers to be confident when dealing with data sharing matters so individuals can be confident their data has been shared securely and responsibly.

As required by the Data Protection 2018, we are working on updating our data sharing code of practice, which was published in 2011. The updated code will explain and advise on changes to data protection legislation where these changes are relevant to data sharing. It will address many aspects of the new legislation including transparency, lawful bases for processing, the new accountability principle and the requirement to record processing activities.

The updated data sharing code of practice will continue to provide practical guidance in relation to data sharing and will promote good practice in the sharing of personal data. In the first instance we will address the impact of the changes in data protection legislation on data sharing and will then move on to developing further case studies. Our intention is that, as well as legislative changes, the code will also deal with technical and other developments that have had an impact on data sharing since the publication of the last code in 2011.

Before preparation of the code the Information Commissioner must consult with the Secretary of State. She is also seeking input from trade associations, data subjects and those representing the interests of data subjects. This call for views is the first stage of the consultation process. We will use the responses we receive to inform our work in developing the updated code.

You can email your response to CentralGovernment@ICO.org.uk

Or print and post to:
Data Sharing Code Call for Evidence
Central Government Department
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire SK9 5AF

If you would like further information on the call for evidence, please email the Central Government team.

Please send us your views by 10 September 2018.

Privacy statement

For this call for evidence we will publish responses received from organisations but will remove any personal data before publication. We will not publish responses from individuals. For more information about what we do with personal data please see our [privacy notice](#).

Questions

Q1 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?

Finding an appropriate lawful basis for data sharing: the inability of the public sector to use the legitimate interests basis is causing problems for sensible non-contentious data sharing, such as to confirm that documents issued by the public authority are valid. This type of data sharing usually involves an organisation providing document details to the public authority for them to confirm that they are genuine and correspond to a document they have issued.

Q2 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

Q3 If yes (please specify)

The code focused on public sector data sharing but there has been an increase in private sector data sharing and in public-private sector data sharing. The code should reflect this.

Q4 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? Please give details.

No

The code should say more about benefits and include consideration of things like:

- What is the detriment to the organisations involved and / or individuals of not sharing the data?
- Is there a greater societal benefit to the data sharing?

Perhaps these could be additional factors to consider (section 5).

One of the barriers to data sharing is the perception that it is inherently 'a bad thing' and an exception, rather than seeing it as just another processing activity that needs to be done appropriately within the right framework.

Q5 If yes in what ways does it achieve this?

n/a

Q6 If no, in what ways does it fail to strike the right balance?

As above.

Q7 What types of data sharing (eg systematic, routine sharing or exceptional, ad hoc requests) are covered in too much detail in the 2011 code?

There is no specific type of data sharing that is covered in too much detail, the code addresses all types equally.

Q8 What types of data sharing (eg systematic, routine sharing or exceptional, ad hoc requests) are not covered in enough detail in the 2011 code?

There is no specific type of data sharing that is covered in too little detail, the code addresses all types equally.

Q9 Is the 2011 code relevant to the types of data sharing your organisation is involved in? If not, which additional areas should we cover?

The code focuses on the public sector but public-private sector data sharing is very common and not really considered.

It would be helpful if the code could provide more examples of data sharing and be clearer about what kinds of data sharing or outcomes are likely to be beneficial, such as fraud prevention, identity verification, improving access to services, providing joined-up services and so on.

GDPR and the DPA 2018 have led to a focus on the minutiae of process and technical legal compliance without looking at what is in the best interests of the individual. This and the inability to use legitimate interests has led to the public sector being terrified to share anything unless there is a watertight legal assessment to guarantee they can. While there of course has to be a lawful basis for sharing, they are being interpreted very narrowly and impacting sensible non-contentious sharing, such as for the aims listed in the previous paragraph.

Q10 Please provide details of any case studies or data sharing scenarios that you would like to see included in the updated code?

As above. Also scenarios such as:

- event organisers asking individuals about dietary or access requirements and passing those details to the relevant parties involved in the event;
- recruitment: sharing candidate details proactively with possible employers; platforms that allow job seekers to upload details and employers to search them;
- venues sharing information between them on individuals banned from their premises;
- public authorities confirming documents or details are valid by checking against their own records (including providing details back as well as a yes / no).

Q11 Is there anything the 2011 code does not cover that you think it should? Please provide details.

It would help to have a template data sharing assessment form and a template data sharing agreement in the same way there are templates for data request forms and data decision forms.

Q12 In what other ways do you think the 2011 code could be improved?

The section on security on page 25 could be expanded and improved. Page 24 has a lot of detail on general security at an organisation but there is little on the security aspects of data sharing arrangements.

A common scenario is for organisation A providing the data to insist that organisation B receiving the data complies with all of organisation A's policies, procedures and standards. This is not feasible and unrealistic and is an especially common approach from public sector bodies.

The code could help by going further than just acknowledging this is an issue by providing solutions, such as a checklist of key points that need to be covered in the receiving organisation's security measures. For example, if an organisation has ISO 27001 or SOC 2, it should be considered appropriate security. If an organisation can show it has policies on things like access control, information classification, change management, supplier diligence, incident management and training, then it should not matter that the content of those policies differs from those of the other organisations involved in the data sharing.

About you:

Q13 Are you answering these questions as?

A private sector worker

Q14 If other please specify:

n/a

Q15 Please provide more information about the type of organisation you work for, ie a bank, a housing association, a school.

A digital identity platform.

Q16 We may want to contact you about some of the points you have raised. If you are happy for us to do this please provide your email address:

Thank you for taking the time to share your views and experience.