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?

- Guidance and examples to show the extent to which good data sharing arrangements, and data sharing agreements in particular, can help demonstrate compliance with GDPR and tying data sharing to the data protection principles. This would include more information on the benefits of data sharing agreements for organisations.
- More guidance around joint controller relationships (even though joint controllers/controllers in common is not a new concept).

- Clarity about when Controller to Controller applies and when Controller-Processor applies.
- A statement that both/all parties involved in the data sharing are equal and have equal accountability in law (even though this should currently be the case).
- Guidance on who is liable if a processor (signed up before GDPR) refuses to accept contract terms required for GDPR.
- Details around what level of detail on breach management and security, etc should be included.
- Guidance on review issues: how often, what should automatically trigger a review, etc.
- Advice on the lawful basis for processing of special category data and what this requires under DPA 2018 (i.e. policy document/statement).
- Advice on the managing the Rights of the Individual across organisations involved in data sharing (e.g. responsibilities/accountability/etc).

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 √

☐ No

Q3 If yes (please specify)

- Larger organisations (especially government bodies) are claiming that DSAs are not necessary if there's a clear legal basis. It would be useful if the code made it clear that these agreements are required (and not just best practice).
- In addition to this, a lack of equality in data sharing relationships, where one organisation is, for example, a government body or provider of funding to the other body. Where there is a clear legal basis for one organisation to receive data, the other organisation

has very little bargaining power around how they want this data to be managed by the receiving party. This means they are often under pressure to send data to another organisation without being assured that the organisation has implemented appropriate technical and organisational measures to ensure a level of security appropriate to the risk, will not onward share, etc.

- Guidance on the extent and scope of 'social protection' law as per Article 9(2)(b) and how this may affect legal justification for DSAs. ICO could produce a register of laws consider social protection and/or social security law as they come to determinations on various laws through casework or court.

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.

☐ Yes √

☐ No

Q5 If yes in what ways does it achieve this?

The code is written in plain English and makes clear the importance of protecting individuals' personal data but also the benefits of data sharing. When it was first published it was an invaluable tool in developing guidance and templates for business to use. The checklists were very useful. It would be very helpful to have example templates of DSAs. Section 14 of the old CoP provided the minimum required to be included in a DSA and was used to develop a template. It would be very useful to see what the ICO considers is a good DSA.

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

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?

Nothing has too much detail. When it comes to this, having detail is vital and the more examples, etc the better. All types of data sharing carry their own risks, so more detail is essential.

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?

- See earlier comments. More examples linking with specific law, including explicit and implicit powers – especially implied powers as this is difficult with law developed decades ago when it was not considered necessary to have explicit data sharing powers built into a Bill.
- More detail on the arrangements to put in place for systematic, routine sharing would also be helpful.

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?

- For public bodies there could be more detail on sharing in the public sector. There's currently 1 page and it mistakenly assumes that bodies derive their power to share from statute.
- More guidance on the law enforcement side of things would be very useful. The old S.29 exemption etc was relatively straightforward, it's currently not clear how this works now with the new Act.
- Guidance on National Security aspects for sharing
- Guidance around safeguarding and sharing of children/adults at risk.
- Absolute clarity on the extent and limits of the 'vital interest' special category condition. Especially when consent to process one person's data is withheld to the severe detriment of another person.

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

- Scenarios covering ad hoc requests from law enforcement agencies, for example police turning up at reception requesting information on an employee. Similarly, for government fraud agencies requesting data and European and government funders requesting data. A degree of pressure is often associated with these 'requests'.
- Government bodies demanding data but not providing legal basis and/or data sharing agreements. The ad hoc requests, one off requests, are common but there is not as much guidance around this.
- Case studies involving medical emergencies and data sharing, especially involving children.
- Case studies where data sharing agreements are used in addition to a contract or examples of how to incorporate data sharing into contractual arrangements.

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

- Data being shared to social media by students and/or staff, and accountability and lines of responsibility.
- Where there are instances of other organisations using network, how agreements between parties are reached
- Home working and BYOD (i.e. sharing of data by a staff member to their personal account) and accountability.
- Use of cloud (SaaS, PaaS, IaaS), transparency and accountability of cloud companies (i.e. should organisations take contracts at face value – difficult to prove/disprove compliance given distribution of services, subcontractors, etc), any certification, etc other than ISO 27001 that we should be looking for, etc?

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

- Example data sharing agreements
- The document is long and could be shortened to make it more accessible, perhaps with supplementary guidance being developed as per the employment CoP. It would also be useful to have a DSA

quick overview guidance document for non-practitioners, allowing the CoP to contain the detail that is required.

- DSA Checklist would be helpful (i.e. what must be included), with a more hard-line approach on requirements e.g. ICO would expect to see xxx as part of your DSA if you were audited.
- Also, including sharing schedule within a DSA to limit additional ad hoc requests by parties resulting in additional unnecessary sharing which drives up risks to privacy of data subjects.
- would be better if further examples/case studies provided and examples of good and bad DSAs.

About you:

Q13 Are you answering these questions as?

- ☐ **A public sector worker √**
- ☐ A private sector worker
- ☐ A third or voluntary sector worker
- ☐ A member of the public
- ☐ A representative of a trade association
- ☐ A data subject
- ☐ An ICO employee
- ☐ Other

Q14 If other please specify:

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

HEFESTIS – part of a not-for-profit Shared Service organisation jointly owned by all Universities and Colleges in Scotland, providing a DPO shared service to further education colleges and to public sector owned bodies.

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:

Point of contact for HEFESTIS:

[redacted]

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