ICO consultation on the draft updated data sharing code of practice

Data sharing brings important benefits to organisations and individuals, making our lives easier and helping to deliver efficient services.

It is important, however, that organisations which share personal data have high data protection standards, sharing data in ways that are fair, transparent and accountable. We also want organisations 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 Act 2018, we are working on updating our data sharing code of practice, which was published in 2011. We are now seeking your views on the draft updated code.

The draft updated code explains and advises on changes to data protection legislation where these changes are relevant to data sharing. It addresses many aspects of the new legislation including transparency, lawful bases for processing, the new accountability principle and the requirement to record processing activities.

The draft updated code continues to provide practical guidance in relation to data sharing and promotes good practice in the sharing of personal data. It also seeks to allay common concerns around data sharing.

As well as legislative changes, the code deals with technical and other developments that have had an impact on data sharing since the publication of the last code in 2011.

Before drafting the code, the Information Commissioner launched a call for views in August 2018. You can view a summary of the responses and some of the individual responses here.

If you wish to make any comments not covered by the questions in the survey, or you have any general queries about the consultation, please email us at datasharingcode@ico.org.uk.

Please send us your responses by **Monday 9 September 2019**.

Privacy Statement

For this consultation, we will publish all responses except for those where the respondent indicates that they are an individual acting in a private capacity (e.g. a member of the public). All responses from organisations

and individuals responding in a professional capacity will be published. We will remove email addresses and telephone numbers from these responses; but apart from this, we will publish them in full.

For more information about what we do with personal data please see our privacy notice.

Questions

Note: when commenting, please bear in mind that, on the whole, the code does not duplicate the content of existing guidance on particular data protection issues, but instead encourages the reader to refer to the most up to date guidance on the ICO website.

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

☐ Yes

☒ No

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

My comments throughout relate principally to the sections and text which seek to explain Data Sharing by, or to, Competent Authorities [CA] under DPA 2018 Part 3 [Part 3].
The complexity of summarising the multiple regimes which apply to data sharing by virtue of the GDPR/DPA 2018 and the specific Part 3 (and associated Schedule 8 provisions) is recognised to be significant, however overall the detail and guidance provided was felt to be sub-optimal or incomplete in the following aspects:
1 – Sharing Data outside the EEA (pg 24) – the specific provisions applicable to Competent Authorities under Part 3 Chapter 5 are not identified here, or indeed referenced.
The LE obligations for such transfers are significantly more burdensome than for other controllers and shall become more restrictive still if Brexit is achieved and the provisions of the Data Protection, Privacy and Electronic Communications (Amendments, etc.) (EU Exit) Regulations 2019 s.37-46 come into effect. These should be properly referenced and a short explanation of the challenges listed here, or in the relevant Part 3 section of the guidance.

2 – Under the sections relating to lawful basis for sharing by Competent Authorities, the threshold to demonstrate a "strictly necessary" in comparison to a merely necessary requirement to share should be clarified or a link to a suitable interpretation of strictly necessary provided.
3 – In the section titled "How do you allow individuals to exercise their information rights in a data sharing scenario?" (pg 51) the guidance makes references to joint data control and Article 26 of the GDPR. It does not however make any reference to the specific obligations for Joint Data Controllers under Part 3 s104, notably the need to designate a lead controller for the purposes of enabling data subjects to exercise their rights. These omissions should be corrected, with suitable text and references introduced here or in the specific Part 3 guidance section.
4 – In the section titled "What is the impact on a data sharing arrangement of requests for erasure, rectification or the restriction of processing?" the references provided only relate to GDPR Articles. The requirements to meet Part 3 Principle 4 (para 4 and para 5) would also appear relevant? Other relevant provisions under Part 3 which are not referenced here should also be added for completeness.
5 – The section titled "What do we need to do about solely automated processing subject to Article 22?" gives comprehensive guidance on the requirements relating to automated processing, but other than a mention that data subjects have a similar right within Part 3 for Law Enforcement processing, no comparable equivalent guidance is given, even though the sections in Part 3 are significant. Consideration should be given to providing suitable references or text to explain these elements.
6 – In the section titled "Law Enforcement Processing: DPA Part3", the content, whilst comprehensive, should potentially make reference (unless it is added elsewhere) to the implications of Part 3 Principle 2 (S.36, para 4) with respect to the limitations which may apply to data collected for a Law Enforcement purpose for any other use – "*Personal data collected for any of the law enforcement purposes may not be processed for a purpose that is not a law enforcement purpose unless the processing is authorised by law*". It is conceivable that this paragraph may restrict or constrain some types of data sharing from Competent Authorities to entities not operating under Part 3 provisions.
7 – In the sub-section titled "We are a competent authority: how do we share data?", the data sharing guidance contains the following text:

'*If you are a competent authority, and the sharing is for law enforcement purposes, then Part 3 may provide a framework allowing you to share data'* – this statement is largely true since Part 3 does describe the measures needed to share data under a Part 3 regime (ie between Competent Authorities, both within EEA and in 3rd countries).

Part 3 does NOT however describe the processes, protocols or regulations to be followed if a Competent Authority processing personal (or sensitive personal) data for a Law Enforcement purpose wishes to share this data with a non-Competent Authority which operates on a non-Part 3 regime.
This is the most complex type of data sharing relationship for a Competent Authority, but underpins public safety measures such as Multi-Agency Safeguarding Hubs (MASH), and interactions with 3rd sector organisations such as Victim Support, Women's Aid, Narnardos and many others.
It is this guidance specifically which is therefore of greatest value and need for the controllers on both sides and its omission should be rectified as soon as possible (though it is recognised that this is not trivial and will require significant work from multiple parties).
The existing CJS data sharing agreements (which the responder played a part in co-creating) falls far short of what is required in the new DPA/GDPR landscape.

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

☐ Yes

☒ No

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

With regard to Law Enforcement processing there are significant gaps detailed in response to Q2 above.
The specific complexities of traversing the legislative boundaries which exist between Part 3 and other DP regimes require further work and may be best handled with a specific document describing these types of data interaction, rather than a single catch-all data sharing code.

The complexities and important role of Policing policies laid down under statute for data processing have been described in two recent court cases [*Bridges v Chief Constable South Wales Police*; and *Catt v United Kingdom*]. These policies which include both the Management of Police Information [MOPI] and Police Security Vetting Policy have implications for the creation of effective data sharing regimes.

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

☒ Yes

☐ No

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

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

☒ No

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

The text provided in earlier responses detail this.

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

☐ Yes

☒ No

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.

The text provided in earlier responses details this.

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

☒ Yes

☐ No

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

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

☐ Yes

☒ No

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

The Law Enforcement Competent Authority data sharing scenarios predominantly describe the lawful basis for non-CA's sharing data to Police and similar Schedule 7 CA's.
These scenarios are the simple use cases, since the powers of Police Constables in Common Law (referred to in detail in recent relevant court cases) tend to provide a firm and established basis for Law Enforcement collection of data from non LE Controllers.
The sharing of data in the other direction is much more complex and poorly covered in this guidance; other than to recognise the need, the public interest of such data being thus transferred and some of the implications of not managing this successfully (specifically the Gangs Matrix database and its compromise).
If a number of representative use cases can be developed as part of a cross-party working group to examine and ratify data sharing from Competent Authorities to Controllers operating under other DP regimes this would go some way to informing and assisting DPO's on all sides as to the relevant suitable measures to be included in data sharing arrangements. Currently many of those in place rely upon practices established under DPA 1998, and as I have described in my response these are unlikely to be suitable in the new regimes and may in fact be unlawful – hence this area requires urgent focussed attention.

Q15 To what extent do you agree that the draft code is clear and easy to understand?

☐ Strongly agree

☐ Agree

☒ Neither agree nor disagree

☐ Disagree

☐ Strongly disagree

Q16 Are you answering as:

☐ An individual acting in a private capacity (e.g. someone providing their views as a member of the public of the public)

☒ An individual acting in a professional capacity

☐ On behalf of an organisation

☐ Other

Please specify the name of your organisation:

Secon Solutions llp

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