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.

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?

(a) Many of the examples provided by the draft code focus on the public sector. For example, in the "*benefits of data sharing*" section starting on page 13, there are three examples of how data sharing can be of benefit but all of them relate to healthcare. There should also be examples of the benefits of data sharing in the private sector (and, more generally, examples relating to the private sector throughout the rest of the document).

(b) Similarly, there is little or nothing in the draft code about how or when it applies in a commercial data licensing context.

(c) The draft code suggests that it does not apply to internal data sharing – see towards the bottom of page 16. This is in contrast to the previous code, which explained that it was still important to consider data protection issues when sharing data internally: "*When we talk about 'data sharing' most people will understand this as sharing data between organisations. However, the data protection principles also apply to the sharing of information within an organisation – for example between the different departments of a local authority or financial services company. Whilst not all the advice in this code applies to sharing within organisations, much of it will, especially as the different parts of the same organisations can have very different approaches to data protection, depending on their culture and functions.*" In our view, much of the draft code continues to be relevant to internal data sharing as well as external data sharing.

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?

In places the draft code provides some detailed advice but in other places it seems to skip over important details. For example:

(a) The questions at the bottom of page 43 (regarding how to assess fairness) are somewhat unhelpful – they are effectively restatements of "is this processing fair?". Some more practical questions might include consideration of: (i) whether there are any adverse impacts on data subjects, and whether those impacts can be justified; (ii) whether the

use of the data is within the reasonable expectations of data subjects or, if it is not, whether the unexpected processing is justified; (iii) whether data subjects were deceived or misled when their personal data was collected; (iv) the balance between the proportionality and necessity of the processing; (v) whether data subjects have any reasonable choice about the processing activity, and the extent to which they can object; (vi) the intrusiveness of the data being used; and (vii) the degree of linkage between the purposes of the processing activity and the purposes for which the data was originally collected.

(b) In the section on transparency (pages 44-45) there is little or no practical advice about how to achieve transparency in a data sharing context. For example, there is nothing about determining which party should provide privacy notices, and no examples of different mechanisms which might be used (e.g. parties giving a single joint notice; or each party relying on its own independent notice; or each party providing a notice which links to the other party's notice).

(c) Pages 50 and 52 refer to the Article 19 requirement to notify recipients of the data about any rectifications, restrictions or erasures except in cases of impossibility or disproportionate effort. It may be helpful to provide examples of when the impossibility and disproportionate effort exceptions might apply.

(d) On page 61 the draft code says, "*In some private sector contexts there are legal constraints on the disclosure of personal data, other than data protection legislation*". It would be helpful if the code could provide some examples of what constraints it is talking about here; for example, is it referring to contractual restraints (i.e. licence restrictions), statutory restraints (e.g. as with the use of the electoral register by credit reference agencies), and/or restrictions under the constitutions of the organisations concerned.

(e) There is nothing in the draft code about whether (or when) it is appropriate for controllers to report personal data breaches to each other. It would be helpful to understand the extent to which the ICO regards this to be appropriate as a matter of best practice in a data sharing context.

(f) Pages 73 and 75 say that an organisation receiving personal data should make appropriate enquiries and checks, including identifying the lawful basis on which the data was obtained. Presumably this is referring to the legal basis on which the data supplier relied when it obtained the data. But (i) it is not clear why the data supplier's legal basis should be relevant to the organisation receiving the personal data, (ii) it is not clear whether this is limited to the legal basis of the

recipient's immediate data supplier or whether the recipient needs to identify the legal basis relied on by every data supplier further up the data supply chain (if there is one), and (iii) it is not clear whether the recipient is expected to evaluate the data supplier's legal basis itself (e.g. to come to its own conclusions about whether the data supplier's processing satisfies the legitimate interests balancing exercise).

(g) On page 74 the draft code says that it is important for both the sharing controller and the recipient controller to do due diligence. It goes on to provide detailed information about what due diligence the recipient controller should do but does not explain what due diligence a sharing controller should do. It does say that "*the organisation sharing the data should follow a similar process,*" but the questions that will need to be asked by a sharing controller will be very different from the questions that are asked by a recipient controller. For example, a recipient controller will primarily need to make enquiries about the provenance and quality of the data, whereas a sharing controller will primarily need to make enquiries about the identity and reputation of the recipient controller, the purposes for which the data will be used, and whether the data will be kept secure.

The same point applies to page 71, where a similar approach has been taken.

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

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.

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.

(a) The requirements for a data sharing agreement (starting on page 26) seem to go beyond the proper scope of a contract. They may have been written with public sector data sharing in mind because they appear to be well out of line with ordinary practice in a commercial context. For example, the draft code suggests that the agreement should record (among other things) (i) why the data sharing is necessary, (ii) the aims and benefits of the data sharing arrangement, and (iii) the legal basis relied on. In our view there is no need for a contract to record these things. The function of a contract is to agree clear and specific legal obligations on each party and (where relevant) to specify remedies for breach of those obligations. Records of the aims and benefits of a data sharing arrangement, and the legal basis on which the parties are relying, can and should go into other documentation such as legitimate interests assessments, DPIAs, Article 30 records, etc. By including unnecessary material in a contract there is a risk of creating unexpected legal obligations such as (i) implied contractual warranties about the factual background set out in the contract, (ii) an implied obligation on a party to achieve the aims and benefits set out in the contract, or (iii) an implied contractual restriction against relying on any legal basis other than those specified in the contract.

(b) For similar reasons, there is no need for a contract to contain a summary of legislative provisions, as suggested on page 29. A contract should not be a source of reference about what the law is.

(c) Page 37 says that organisations must identify "at least one" legal basis for sharing data. This suggests that there can be more than one legal basis for a particular processing activity, which is in line with the GDPR and other ICO guidance. However, elsewhere in the document there are clear implications that there will be only be one legal basis for processing – e.g. page 39 says that an organisation "should decide which lawful basis applies" and should "choose the appropriate lawful basis from the start". It goes on to advise against swapping to "a different lawful basis". It is not clear how this is supposed to work where more than one legal basis is available.

(d) On page 38, the description of the legitimate interests legal basis seems odd, particularly the use of the word "protect". Personal data can be "protected" even when it is being processed on the basis of legitimate interests.

(e) Pages 47 to 48 contain some material relating to appropriate due diligence in a security context. Some of this will not always be appropriate. There are instances of data sharing where it will not be possible for a data supplier to perform due diligence into the way a data recipient will handle data after it has been supplied (see page 48), such as where data is requested by a regulator under a legal power to gather information. Also, it may be useful to cross-refer between this section and the section dealing with due diligence on pages 74-75.

(f) On page 21, "harm" should refer to "physical harm", and it may be sensible to refer to the ICO's list of circumstances in which a DPIA is mandatory.

(g) On page 29 it is not clear who "the people concerned" are. Is this referring to data subjects or to the parties to the data sharing arrangement?

(h) In various places the draft code refers to further information available on the ICO website but links only to the ICO home page at www.ico.org.uk. If possible, it would be more helpful to link directly to the relevant page(s) within the ICO website.

(i) At the top of page 45, it is unclear what "*commence new data sharing*" means in this context. Perhaps this should say "*commence new types of data sharing*".

(j) The top of page 45 says that an organisation must give privacy information "directly" to individuals. There appears to be no basis for this. Information can be provided to individuals through third parties; and information does not need to be provided at all if the individuals already have it (e.g. from a third party) or where the controller can demonstrate that providing the information is impossible or involves disproportionate effort.

(k) Page 53 says that if a data sharing arrangement involves any automated decision-making, the specific lawful basis for that automated decision-making must be documented in the organisation's data protection policy. There does not appear to be any basis for this; the lawful basis could just as well be recorded in the organisation's Article 30 records, for example.

(l) The reference to providing privacy notices on page 75 (under "*What else do we need to do?*") should be qualified with the words "*unless an exemption or exception applies*". This approach has been taken elsewhere in the draft code – see pages 5, 42 and 44.

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:

TransUnion Information Group

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