Take care before you share: the ICO's draft Data Sharing Code of Practice

November 2019

A version of this article was first published in the Privacy Laws & Business UK Report, Issue 106 (November 2019).

Summary

In July, the Information Commissioner's Office ('ICO') published a draft Data Sharing Code of Practice ('the code'). This is a noteworthy piece of draft guidance as it will have wide-ranging application. In addition, much has changed in the data protection world since the current Data Sharing Code of Practice was published in 2011. Now is therefore a good time for organisations to review their approach to data sharing.

Whilst much of the code contains helpful guidance, it is likely to be challenging to follow in its current form in all circumstances. A number of organisations, including the City of London Law Society, submitted comments to the ICO during the consultation period for the code, which closed on 9 September. It is hoped that these comments will be taken into account by the ICO to make the final version of the code as useful as possible.

Background on the code

The ICO is required to prepare the code under s.121 of the Data Protection Act 2018 ('DPA'). The code must contain practical guidance in relation to the sharing of personal data in accordance with the requirements of data protection legislation and such other guidance as the ICO considers appropriate to promote good practice.

The code will be admissible in legal proceedings and the DPA obliges a court or tribunal to take account of it, if it appears to be relevant to the question before them. The Information Commissioner is similarly required to take account of the code when exercising her functions under data protection law.

In light of this, it would be helpful for organisations if the code could distinguish more clearly between guidance that explains the legal requirements and optional good practice recommendations that, as the ICO state, "*aim to help [you] adopt an effective approach to data protection compliance*".

Structure of the code

The code is significantly longer and more wide-ranging than its predecessor. For example, it includes new sections on accountability, data sharing and children, data ethics and data trusts. The code contains more examples and case studies, and also contemplates the inclusion of checklists and template forms, which the ICO plans to add to the final version.

Key points of interest

The code contains a significant amount of useful and welcome guidance. Conscientious organisations that were already complying with best practice will find it easier to follow than others who are still grappling with general compliance issues, but even then, in some circumstances, the code's guidance may be impractical. For example, if the code stays in its current form, data sharing agreements in respect of even the most innocuous data sharing would appear to need lengthy documents with detailed explanations embedded within. As a whole, the code is also currently very focussed on the public sector which may be disappointing to a number of private sector organisations. Some of these concerns, and other key points of interest about the code, are considered below.

Nature of data sharing

The ICO recognises that data sharing can include routine and scheduled data sharing as well as on an urgent one-off basis, but there is little mention of data sharing that falls somewhere in between the two. For example, in the context of private sector commercial transactions, data may be shared once or a few times, but not necessarily as a matter of urgency. In addition, the majority of case studies and examples relate to the public sector. Some organisations may interpret this to mean that the code is less relevant to them, but this would be a mistake as the majority of the code is relevant to all data sharing.

Data sharing agreements

Unsurprisingly, the ICO recommends that as a matter of good practice, businesses sharing data should put in place a data sharing agreement. Not only will this help them with their accountability obligations under the GDPR, it will also help all parties be clear about their respective roles, set out the purposes of the data sharing, cover what is happening to the data at each stage and set standards.

The code states that a data sharing agreement should include provisions to deal with various practical problems that may arise when sharing data, such as:

- being clear about which datasets the parties can share to prevent irrelevant or excessive information being disclosed;
- provisions on accuracy of shared data, for example by requiring a periodic sampling exercise;
- mandating compatible datasets and recording data in the same way;
- setting common rules for the retention and deletion of shared data and procedures for dealing with cases where different statutory or professional retention or deletion rules apply;
- common technical and organisational security arrangements, including the transmission of the data and procedures for dealing with any breach of the agreement;
- procedures for dealing with access requests, complaints or queries;
- timescales for assessing the ongoing effectiveness of the arrangements; and
- procedures for dealing with the termination of the data sharing initiative, including the deletion of shared data or its return to the organisation that supplied it originally.

Until the ICO produces a comprehensive checklist in its final version, this is likely to be a useful starting point for some of the provisions that should be included in a data sharing agreement, albeit not all will be appropriate in all circumstances.

In addition, the code sets out some further provisions that the ICO would expect to see in data sharing agreements. These include:

- an explanation of why the data sharing initiative is necessary;
- the specific aims of the parties;
- the benefits the parties hope to bring to individuals or to society more widely by such sharing data;
- extracts of relevant legislation; and
- a clear explanation of the lawful basis.

It will undoubtedly help organisations to meet their accountability obligations if much of this analysis is agreed between the parties and documented clearly. However, it is not as obvious that a data sharing agreement is the most appropriate place for this analysis to be recorded. Other suitable logs for this could include data protection impact assessments, records of processing and/or legitimate interest assessments.

Joint controllership

The code briefly mentions joint controllership and the requirements of Article 26 of the GDPR for joint controllers to put in place a 'transparent arrangement' (which can be met by way of a data sharing agreement). However, it isn't entirely clear how such an arrangement would then differ from an agreement between independent controllers. The code appears to require this in respect of all controller-to-controller data sharing, whether or not Article 26 applies.
In addition, parts of the draft code seem to imply that data sharing renders the participants joint controllers (e.g. where it states that it is good practice to provide a single point of contact for individuals rather than making multiple requests to several organisations with which their personal data has been shared). We suspect this is unintentional and, given the ongoing confusion about when a joint controllership may arise following the recent decision in the Fashion ID case (Case C-40/17), hopefully this will be clarified in the final version.

Liability issues

One area of uncertainty that organisations often grapple with is around the interaction between Article 82 of the GDPR and the limits on liability agreed between parties in a data sharing agreement. Article 82 provides individuals with the right to compensation for damage suffered as a result of a breach of the GDPR. It also allows a controller to claim back from another controller the part of the compensation corresponding to that other controller's responsibility for the damage. Most organisations currently take the view that any contractual limitations (such as liability caps) agreed between parties, including between controllers, would restrict what could be claimed under Article 82 and it would be helpful if the ICO were to acknowledge this in its final version.

M&A and due diligence

The ICO confirms that the code applies to data sharing in the context of M&A. However, the M&A section is very generic and does not explore in any detail the privacy concerns that will likely come up at different stages of an M&A transaction (e.g. due diligence, integration planning, completion). The M&A section is also slightly confused as it mixes up concepts from share and asset sales and so does not provide practical guidance on the areas it does refer to. This lack of clear guidance on some routine challenges that arise in an M&A context can hopefully be rectified in the final version.

The section on sharing personal data in database lists, however, includes a useful checklist of due diligence questions that an organisation receiving

data should ask of its counterparty (see the box below). Although this section appears to be aimed at certain types of data sharing (e.g. sharing by data brokers, marketing agencies, credit reference agencies, clubs and societies and political parties) rather than M&A, the questions below are also likely to be relevant in the context of a business acquisition where the assets being bought include personal data, such as a customer database.

The code states that organisations receiving a database of personal data should make appropriate enquiries and checks, including:

- confirming the source of the data;
- identifying the lawful basis on which it was obtained;
- checking what individuals were told at the time (including reviewing any privacy notices);
- verifying details of how and when the data was initially collected;
- checking the records of consent, if *relevant;*
- checking that the data is accurate and up to date; and
- ensuring that the data received is not excessive or irrelevant.

Data sharing in a litigious context

It is interesting that the code is silent on certain types of sharing such as in the context of disputes, regulatory investigations and litigation. Some of the code's recommendations will be impractical in these contexts.

For example, a regulator is unlikely to agree to enter into a data sharing agreement with a company involved in an investigation. It would be helpful if the ICO were to acknowledge this in the code.

Data ethics

The code includes a new section on data ethics which provides guidance on the ethical principles that should be considered when deciding whether to share data, in addition to lawfulness and the technical requirements of data sharing. This could be read as imposing an additional layer of obligation on businesses and would also create uncertainty, as general principles around the ethical use of data are still in development. Having said that, it is likely that a number of the factors the ICO raise in relation to data ethics would be relevant to any general assessment of fairness that a business has to carry out under the GDPR and so should certainly not be dismissed as irrelevant.

Next steps

The final version of the code must be submitted to the Secretary of State and then laid before Parliament for approval within 40 days.
The ICO hasn't indicated a deadline for when it will be ready to submit the final version to the Secretary State, but it is hoped that this will happen before the end of the year or early 2020.

For businesses, despite the fact that this is only a draft code, the direction of travel is clear and not entirely unexpected. This code builds on a number of recommendations that were included in the 2011 guidance and that businesses should already have been following. For example, it is difficult to see how businesses can avoid having to put in place data sharing agreements in today's post-GDPR world, nor why they would wish to, given how far they can go to help meet general compliance and accountability obligations under the GDPR, as well as to allocate liability and hence mitigate risk.

Organisations should consider taking the following steps now, to the extent they haven't already:

- mapping external and internal data flows to understand where data sharing occurs (as opposed to where data processors are engaged) and why. This applies both to data sharing within a corporate group structure or with third parties;

- assessing the implications of the Fashion ID case and determining which instances of data sharing may amount to joint controllership;

- identifying where data sharing agreements should be entered into and on what terms; and

- commencing a high level review of existing data sharing agreements. Whilst the final version of the code will provide more definitive and additional guidance (including a checklist of provisions), it should still be possible to categorise agreements into broad categories of risk at this stage, depending on the extent of the provisions that are included.

This article was written by Rebecca Cousin and Cindy Knott. Slaughter and May advises on all aspects of data protection and Privacy. Please contact us if you would like any further information. Further publications are available on our website.

Rebecca Cousin
T +44 (0)20 7090 0000
E rebecca.cousin@slaughterandmay.com

Cindy Knott
T +44 (0)20 7090 5168
E cindy.knott@slaughterandmay.com