EMW CONSULTATION RESPONSE TO THE DATA SHARING DRAFT CODE OF PRACTICE

FRIDAY 6 SEPTEMBER 2019

SUMMARY

This document sets out EMW Law LLP's (**"EMW"**) consultation response to the ICO's Data Sharing Code of Practice draft for consultation, dated 15 July 2019 ("**Draft Code**").

We welcome the Draft Code and the clarity it brings to certain data sharing issues that have arisen post-GDPR. However, we also criticise the Draft Code for going too far, both legally (its effect is to impose obligations on businesses which are simply beyond the requirements of the GDPR and DPA) and practically (many of the requirements imposed are unworkable for some businesses). The Draft Code also seems to focus its examples far too heavily on public sector entities and fails to take into account the vast impact it will have on the private sector, particularly those businesses for whom data sharing is a daily practice.

Our concerns can be summarised as this:

- The authors of the GDPR considered it necessary to mandate requirements that must be set out in a written agreement between controllers and processors. There is no equivalent regulatory (or statutory) imposition on controller to controller agreements. All of the ICO's guidance on data sharing must be viewed through that lens. The general use of statements using words such as "shall", "must" or "should" when describing data sharing duties gives the impression that these statements are mandatory (in effect, the law) when that is simply not true. They are good practice recommendations and the Draft Code should be more clear about this. Only a few passing references are made to this point.
- At times, the Draft Code is simply unworkable, placing disproportionate burdens on UK businesses which are not required by law. This impact will be most acutely felt by SMEs, although even business with large legal functions are likely to struggle to meet all standards and expectations in the Draft Code.

Deciding to share data

Draft Code		Our Response
Page No.	**What your Draft Code says**	**What we think you should do**
20	"We recommend you consider following the DPIA process, even where you are not legally obliged to carry one out".	If it is not a legal requirement to carry out a DPIA how can the guidance recommend that a DPIA should be conducted? This is extremely onerous and very likely to be misinterpreted. Organisations, whether small or large, are unlikely to be able to comply with this. It is impractical. This sentence should be deleted or replaced with the following: "*We recommend that, if you are unsure about whether a DPIA is or could be needed, you follow the DPIA process".*
23	"**Who requires access to the shared personal data?** You should employ "need to know" principles, meaning that you should only share data to the extent that it is proportionate to do so: • other organisations should only have access to your data if they need it; and • only relevant staff within those organisations should have access to the data. As part of this, you should consider any necessary restrictions you may need to impose on the onward sharing of data with third parties."	This is new and not required under the GDPR. The second bullet point in particular may be onerous to put in place and police. Is it required? By using the words "should" you give the impression this is a legal requirement, which is not the case.

Data sharing agreements

Your Draft Guidance		Our Response
Page No.	**What your Draft Code says**	**What we think you should do**
25	"It is good practice to have a data sharing agreement".	This section gives the reader the impression that entering into a data sharing agreement is merely good practice, as opposed to mandatory. However, under the section 'What should we include in a data sharing agreement?', it is stated that to comply with legislation organisations are expected to cover certain points within a data sharing agreement. • Is a data sharing agreement mandatory or not? Please answer this point directly in the Draft Code. • If not, do the additional obligations which are obligatory to cover within a data sharing agreement fall away? Put another way, are the additional obligations (purpose of data sharing, other organisations involved in data sharing, and sharing with another controller, etc) mandatory if a sharing agreement or similar is not present? • Please confirm if your Draft Code of practice is intended to have retrospective effect, meaning that controllers are required to revisit data sharing agreements entered into prior to the Draft Code taking effect to insert or remove clauses which are not in keeping with your Draft Code.
25	"A data sharing agreement: helps all the parties to be clear about their respective roles; sets out the purpose of the data sharing; covers what is to happen to the data at each stage;	With reference to a data sharing agreement setting "standards", it would be helpful to expand as to what a sharing agreement sets the standards of or for.

	and sets standards".	Furthermore, it may be beneficial to expand on all the points in this paragraph.
26	"Drafting and adhering to an agreement does not in itself provide you with any form of legal indemnity…"	This paragraph should not use the term, 'legal indemnity', but paraphrase in normal language. We think it should say: "Having a data sharing agreement in place may help prevent breaching data sharing laws but does not itself make any of the parties immune from breaching such laws and the consequences of doing so'.
26	"In order to adopt good practice and to comply with the data protection legislation, the ICO expects you to address a range of questions in a data sharing agreement, including: **What is the purpose of the data sharing initiative?** Your agreement should explain: • why the data sharing initiative is necessary; • the specific aims you have; and • the benefits you hope to bring to individuals or to society more widely. You should document this in precise terms so that all parties are absolutely clear about the purposes for which they may share or use the data."	Reference to needing to address a range of questions in a data sharing agreement in order to comply with the data protection legislation is incorrect. The data protection legislation does not require these questions to be addressed nor does it require that controllers have a data sharing agreement in place. The words "and to comply with data protection legislation" should be removed. There is reference to 'you should' document this suggesting it is mandatory. However, as referred to above, the Draft Code refers to a data sharing agreement being good practice rather than mandatory. It should be clarified whether this really is a 'should' and mandatory or not. Further guidance is required around this so that organisations know exactly what should be included. Examples would also be useful.
27	"**What is our lawful basis for sharing?** You need to explain clearly your lawful basis for sharing data."	This is new and is not required under the data protection legislation. Why do the parties need to document their lawful basis in an agreement? Controllers are already

		under an obligation under the GDPR to have a lawful basis for processing data and this will form part of their internal compliance. Requiring them to specify the lawful basis in the data sharing agreement is excessive. Following on from the point above, what are the implications if the other party to a data sharing agreement specifies a lawful basis which is likely to be incorrect. Are the other parties to the data sharing agreement required to clarify and correct these issues? Or is it acceptable for them to assume that the other controller's identified lawful basis is correct?
27	" You must document the relevant conditions for processing, as appropriate under the GDPR or the DPA, if the data you are sharing contains special category data or criminal offence data under the GDPR, or sensitive data within the meaning of Parts 2 or 3 of the DPA."	Use of the word 'must' suggests this is mandatory. However, throughout the Draft Code it suggests that data sharing agreements are good practice. This should be clarified.
27	"You should set out procedures for compliance with individual rights. This includes the right of access to information as well as the right to object and requests for rectification and erasure. The agreement must make it clear that all controllers remain responsible for compliance even if you have processes setting out who should carry out particular tasks. For example, the agreement should explain what to do when an organisation receives a request for access to shared data or other information, whether it is under the data protection legislation, FOIA or the EIR. In particular, it should ensure that one staff member (generally a DPO) or organisation takes overall responsibility for ensuring that the individual can gain access to all the shared data easily "	The Draft Code states that the agreement '*must make it clear that all controllers remain responsible for compliance even if you have processes setting out who should carry out particular tasks*'. If a data sharing agreement is not mandatory, why 'must' it state this? Further guidance is required around the requirement to have procedures in place. The controllers will already have their own procedures for dealing with data subjects exercising their rights so this does appear to be excessive. It is unlikely that any organisation will allow the other party to a data sharing agreement to take overall responsibility for ensuring that the individual can gain

		access to all shared data. This may be appropriate for a joint controller relationship, but that is not what your Draft Code is referring to. Given the potential for reputational damage, there is no way an organisation will want to handover responsibility over to the other party. This is also unlikely given the potential exposure under GDPR if the request is not dealt with correctly – given both parties will be controllers and have their own obligations and responsibilities under GDPR.
28	"**What information governance arrangements should we have?** Your agreement should also deal with the main practical problems that may arise when sharing personal data. This should ensure that all organisations involved in the sharing: • have detailed advice about which datasets they can share, to prevent irrelevant or excessive information being disclosed; • make sure that the data they are sharing is accurate, for example by requiring a periodic sampling exercise; • are using compatible datasets and are recording data in the same way. The agreement could include examples showing how particular data items should be recorded, for example dates of birth; • have common rules for the retention and deletion of shared data items and procedures for dealing with cases where different organisations may have different statutory or professional retention or deletion rules; • have common technical and organisational security arrangements, including the transmission of the data and procedures for dealing with any breach of the agreement;	This appears to be overly onerous and goes beyond the requirements of the GDPR. It would be inappropriate to require this level of detail where there is routine and/or low risk data sharing occurring. Many organisations that share data on a daily basis will not be able to comply with these requirements. It is unlikely, for example, that both controllers will use the same methods for recording data and may not have common rules for retention and deletion of shared data or common technical and organisational security arrangements (particularly where there is disparity between the 2 parties, such as an SME and a PLC). Again, there is reference to 'should' suggesting this is mandatory. This should be changed to 'may'. What qualifies as detailed advice regarding datasets that can be shared? This section, overall, makes it unclear as to whether a data sharing agreement is a legally obligation. Furthermore, the points set out to be covered in the data

	• have procedures for dealing with access requests, complaints or queries from members of the public; • have a timescale for assessing the ongoing effectiveness of the data sharing initiative and the agreement that governs it; and • have 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.	sharing agreement appear to be onerous and unclear as to how to achieve the suggestions in practice, particularly for SMEs. For example, requiring a small company or SME to conduct period sampling of data to check accuracy seems impractical if not unachievable. This is compounded by the fact that, as drafted, a sharing agreement is not mandatory in the first place.
29	"**What further details should we include?** […] • a summary of the key legislative provisions, for example relevant sections of the DPA, any legislation which provides your legal power for data sharing and links to any authoritative professional guidance; • a model form for seeking individuals' consent for data sharing; and • a diagram to show how to decide whether to share data."	Why would it be necessary to set out legislative provisions? These are already set out in the legislation and so it feels unnecessary to repeat them in the data sharing agreement. Each controller is likely to have its own consent wording. Why is it necessary to have a model form? Again, a diagram to decide whether to share data seems unnecessary. This would have already been considered prior to the agreement and goes beyond GDPR.

Security

Your Draft Guidance		**Our Response**
Page No.	**What your Draft Code says**	**What we think you should do**
47	"it is essential that all of your staff involved in data sharing understand the importance of protecting personal data".	This statement is unqualified. We think it should read as follows: "it is essential that all staff involved directly in

		data sharing are aware of your responsibility to protect personal data and, in particular, what their responsibilities are when carrying out functions connected directly to the sharing of data".
47	"you should check that the same applies across the organisation you are sharing data with".	This statement is not qualified and goes beyond the requirements of the GDPR. It fails to explain what steps an organisation should take to administer these checks, what the parameters of these checks are or why it is deemed necessary to undertaken them when there is no direct duty in the GDPR to this affect. In particular: 1. as regulator, do you agree that it is reasonable for the entities simply to enter into contractual terms that confirm that their staff are aware of the importance of protecting personal data, or are further investigative steps required? 2. is it reasonable to expect businesses to inspect, monitor or even audit staff at the organisation receiving the personal data? How far does the duty to "check" extend? In practical terms, what does it involve?
48	"Organisations that you share data with take on their own legal responsibilities for the data, including its security. However, you should still take reasonable steps to ensure that the data you share will continue to be protected with adequate security measures by the recipient organisation:	The first sentence of your paragraph (quoted) is a correct statement portraying the requirements set out in the GDPR and DPA. The sentences that follow in our view go beyond what is required in the GDPR and DPA. In particular:

	• ensure that the recipient understand the nature and sensitivity of the information; • take reasonable steps to be certain that the security measures are in place, particularly to ensure that you have incorporated an agreed set of security standards into your data sharing agreement, where you have one;	1. regarding the first bullet point, please see our comments above regarding page 47; 2. please provide examples of what you consider to be reasonable steps (second bullet point) ? Unless the ICO provides more detailed guidance and examples, the requirements that you set out here are likely to place a significant time and cost burden on businesses as they try to undertake checks where doing so is unnecessary and beyond the requirements of the law.
51	"In a data sharing arrangement, you must have policies and procedures that allow data subjects to exercise their individual rights."	The use of the word "must" suggest that this is mandatory. The GDPR and DPA do not make it mandatory. We recommend changing this to "may". The Draft Code also fails to explain what the nature of these policies and procedures is. It could be read a number of ways: 1. does it mean having an informal undertaking between controllers regarding data subject rights? 2. is it acceptable for both controllers to simply declare in the data sharing agreement that they will comply with their legal requirements under the law and deal directly with data subjects, rather than entering (perhaps unnecessarily) into dialogue with other controllers with whom personal data has been shared? 3. does it mean that more detail is required than

		suggested by (2) above, but that contractual clauses only will be sufficient for the parties provided they at least include clauses which document the essence of what will happen in practice, namely that one party is primarily responsible for dealing with data subjects exercising their rights? 4. does it mean that, for each commercial agreement where data is shared, the parties must also set about negotiating and finalising separate policies between them which detail how data subject rights are to be exercised? If so, is it proportionate to expect businesses and industries to bear the cost and time that the creation of such policies and procedures will inevitably incur?

Due Diligence when sharing data following mergers and acquisitions

Your Draft Guidance		**Our Response**
Page No.	**What your Draft Code says**	**What we think you should do**
71	"ensure that you document everything you do with the data";	Please confirm, practically, what the ICO means in respect of use of the word 'everything'. This is clearly excessive and disproportionate, even when considered in light of Article 30 GDPR (which does not contain a requirement to document everything.)

		Can the ICO provide examples of certain things that would not have to be documented i.e. if data is accessed (and discussed verbally) for legitimate purposes as part of any DD carried out as part of the response to a particular buyer enquiry. Likewise could the ICO provide examples of typical matters arising with use of data that must be documented. Please confirm the ICO's position in respect to any restraint of trade / reorganisation as a result of the administrative burden of document 'everything' that is done with personal data.

EMW LAW LLP

MILTON KEYNES

6 SEPTEMBER 2019