The City of London Law Society

4 College Hill
London EC4R 2RB
Tel +44 (0)20 7329 2173
Fax +44 (0)20 7329 2190
DX 98936 - Cheapside 2
mail@citysolicitors.org.uk
www.citysolicitors.org.uk

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

By e-mail only: - datasharingcode@ico.org.uk

City of London Law Society Data Law Committee

Submission to the Information Commissioner's Office on the draft Data Sharing Code of Practice

1. Introduction

The City of London Law Society ("CLLS") represents approximately 17,000 City lawyers through individual and corporate membership including some of the largest international law firms in the world. These law firms advise a variety of clients from multinational companies and financial institutions to Government departments, often in relation to complex, multijurisdictional legal issues. The CLLS responds to a variety of consultations on issues of importance to its members through its' 19 specialist committees.

This submission has been prepared by the CLLS Data Law Committee (the "Committee"). We welcome the opportunity to respond to the Information Commissioner's Office's (the "ICO"'s) public consultation on the draft Data Sharing Code of Practice (the "code"). The CLLS recognises the importance of data sharing as a topic of very broad application: almost every controller will be sharing data and so issues surrounding data sharing arise very regularly for our clients in practice. As such, we welcome the expansion of the ICO's guidance and know that it will be of great assistance to data protection practitioners dealing with these issues on a day-to-day basis.

Given the importance of this guidance, we have undertaken a detailed review of the current text. The first part of our response contains some high level comments on the code as a whole and the second part contains more granular commentary on the text of the current draft. As we have sought to provide detailed commentary on all aspects of the code, we have not aligned our response to the consultation survey prepared by the ICO. However, we have sought to answer the questions posed throughout this response paper. If it would be of assistance to the ICO we would, in addition, be happy to provide responses to the survey questions directly.

It is worth saying, finally, that our response paper has focused on the areas of the code that we consider would benefit from some amendment and we have not listed in the same way the large number of areas in the current draft that we think are good and right. This could give a wrongly negative impression that we want to rectify: we greatly appreciate the ICO's work on the current draft code and believe it is a very good starting point.

We do hope that our feedback will be of value to the ICO in finalising the code. If it would be useful for the ICO to discuss with us any or all of the points made, one or more representatives of the Committee would be very happy to meet with the ICO.

Unless otherwise stated, references to Articles, Recitals and Chapters are to articles, recitals and chapters in the GDPR, and references to paragraphs and sections are to paragraphs and sections in the code.

2. General comments

2.1 Structure of the code

(A) As the ICO strive to make their guidance user friendly, the ICO may wish to consider making a few amendments to the structure of the code to make it clearer and more readable:

(i) The code sections could potentially be reordered to better reflect the order in which issues arise in a data sharing arrangement. For example, controllers will need to understand their various GDPR obligations before drafting their data sharing agreement. The code sections could therefore be ordered as follows:

(a) introductory sections (including "About this code" for example);

(b) data protection principles (including the current p. 31 – 61 as well as the section on data ethics, discussed below);

(c) data sharing agreements; and then

(d) specific types of data sharing (such as data sharing and children).

(ii) The summary may benefit from sub-headings to make it more easily digestible.

(iii) The "What is the purpose of this code?" paragraph on p. 11 may make an excellent introduction to the code and could therefore potentially be moved to p. 7.

2.2 Nature of recommendations in the code

(A) As the current draft appears to suggest that some requirements in the code are close to mandatory, whereas others are more optional recommendations for

good practice, it would be very helpful if the ICO provided further guidance on the nature of the recommendations included in the code.

(B) For example, in the "About this code" section on p. 8, a distinction is drawn between:

(i) parts of the code containing "practical guidance on how to share data fairly and lawfully, and how to meet your accountability obligations" which "will help you comply with your legal obligations"; and

(ii) parts of the code providing "optional good practice recommendations, which do not have the status of legal requirements, but aim to help you adopt an effective approach to data protection compliance."

(C) The ICO may therefore wish to consider distinguishing, by formatting for example, which recommendations:

(i) are considered sufficiently fundamental that a failure to adopt the requirement would likely constitute a breach of the GDPR; and

(ii) which are optional good practice recommendations only.

(D) The ICO may also wish to review the language used in the code to describe what controllers need to do, as this may help to clarify which provisions are optional good practice recommendations and which are mandatory. In some places in the code, the phrase "you should consider" is used, on p. 75 for example, and this seems to us to be the correct tone for the ICO to adopt in relation to all but the most mandatory requirements. Conversely, the phrase "you should", which is currently used in quite a few places (notably in the data sharing agreements section) may be better reserved for obligations that are entirely mandatory.

2.3 Scope of the code

(A) We can see that the ICO have endeavoured to provide a comprehensive guide to the considerations that organisations would need to bear in mind ahead of data sharing. However, we wonder whether, given the statutory nature of the code and its potential role in enforcement actions, some of the points made in the code may be better made through other means, such as on the ICO's blog. The ICO's Brexit materials have helpfully been spread across a number of documents in different formats, including blogs and FAQs, and the ICO may wish to take similar approach to its materials on data sharing. This would also help ensure that the code doesn't become too long a document.

(B) We acknowledge that the Commissioner is given a wide discretion in s. 121(1) Data Protection Act 2018 ("DPA 18") as to what to include in the code, including both:

(i) practical guidance in relation to data sharing in accordance with data protection legislation; and

(ii) such other guidance as the Commissioner considers appropriate to promote good practice in the sharing of personal data (with "good practice in the sharing of personal data" being broadly defined with reference to the Commissioner's discretion in light of data subjects' and others' interests, as well as compliance with data protection legislation).

(C) However, given that the a court or tribunal "must take into account" relevant provisions of the code in determining a relevant question before the court (under s. 127(4) DPA 18), the ICO may wish to consider whether the following points and sections are sufficiently closely connected with data sharing under data protection legislation and the promotion of good practice in data sharing to warrant inclusion in this statutory code rather than elsewhere in the ICO's online resources:

(i) in the "What is the purpose of this code?" section, the "Common concerns about data sharing" and "The benefits of data sharing" sections and accompanying examples (on p. 11 – 15);

(ii) in the "What about access and individual rights?" paragraph at the bottom of p. 27, the requirement for a data sharing agreement to explain what to do in relation to requests for access under the FOIA and EIR regimes;

(iii) in the "What about access and individual rights?" paragraph at the bottom of p. 28, a suggestion that public authorities' data sharing agreements address the inclusion of certain types of information from their FOIA publication scheme;

(iv) in the section on "What factors should we consider?" (ahead of data sharing) on p. 23, the factor titled "How can we check the sharing is achieving its objective?" which appears to be driving at commercial considerations;

(v) in the section on "What documentation do we need to keep?" on p. 34, the reference to records of personal data breaches; and

(vi) in the section on "Data ethics and data trusts", the paragraph headed "What has been happening in the area of data ethics?", on p. 85.

2.4 Types of data sharing covered by the code

(A) We welcome the useful distinction drawn by the code between:

(i) routine data sharing; and

(ii) ad hoc, urgent data sharing.

However, it would be very helpful if the guidance could address that data sharing in commercial transactions often does not fit neatly into either of these categories: being neither routine nor really urgent, particularly in light of the

public sector emergency examples given on p. 81. Although ad hoc and urgent/emergency data sharing situations are dealt with separately early in the code (such as on p. 18), they appear later to be conflated (such as on p. 80, when routine data sharing is juxtaposed with urgent data sharing only). It would therefore be useful if the ICO could provide some further clarification as to how the code applies to non-urgent ad hoc data sharing.

(B) It would also be helpful if the code clarified that the urgent/emergency situations referred to in the code involve risk to life and public safety and do not include business emergencies, if this is the ICO's view.

(C) Our view is that many data sharing scenarios fall into a continuum between one-off and routine sharing. For example, in an M&A context the data sharing is not routine, but often includes several episodes of data sharing as the transaction progresses: some data will initially pass from seller to purchaser in the due diligence phase, with further sharing in the integration and completion phases. Such data sharing is not routine or unexpected, and is often not urgent.

(D) Other examples of data sharing that fall into this continuum arise in the context of disputes (where data will be disclosed to a court) and regulatory investigations. For example, a private sector organisation may, on request, disclose data to financial, competition or other regulatory bodies in the context of an investigation. The issues and considerations that will be relevant in this type of situation (and in the context of litigation) will differ to a certain extent from the ones generally mentioned in the code. For example, it would be rare for a regulator to agree to enter into a data sharing agreement with the organisation they are investigating. The ICO may therefore consider that it would be beneficial to acknowledge this in the code. It is worth noting here that a number of these regulators rely on statutory powers to request information from organisations and have established guidance and practices when carrying out their work. It may be helpful for the ICO to liaise with such bodies as further guidance is developed, to enhance consistency and certainty for organisations wishing to be as compliant as possible. If it would be useful for the ICO to discuss this particular situation in more detail, one or more representatives of the Committee would be very happy to meet with the ICO.

(E) The ICO may wish to consider including an explanation as to how the code should be interpreted and applied to in-between scenarios, such as those referred to in (C) and (D) above. Without further clarification, there may be a risk that organisations may conclude that their data sharing activities fall outside the types of sharing represented in the code, and therefore that the code does not apply. We note that the current draft confirms, on p. 71, that the code applies to data sharing in M&A transactions, however such confirmation is not currently given for other commercial transactions.

(F) The code briefly discusses data pooling (on p. 18), but does not explain whether this falls within the other two categories of data sharing or forms a third type. It would be helpful if this was clarified and the section on data pooling was expanded.

(G) The ICO may also wish to reflect in the code that the volume and sensitivity of data shared between the parties could affect how the code applies, in addition to the distinction between routine and ad hoc data sharing. For example, where two businesses are working together on a joint project, the business contact details of the employees involved from each party may be exchanged but no other personal data may pass between the parties. Such circumstances could involve routine data sharing between the two parties, but only a very small amount of non-sensitive personal data is actually being shared. In this instance, it seems disproportionate for the parties to need to comply with the full range of obligations in the code relating to data sharing agreements and audit etc.

2.5 Impact of the code on liability between controllers

(A) We would welcome guidance in the code as to how Article 82 interacts with the provisions on liability that are typically included in data sharing agreements.

(B) As we understand Article 82(4), the ability for a data subject to recover all compensation from one controller is not limited to joint controller scenarios, but also applies to data sharing scenarios (although the scope of Article 82 is not entirely clear). Again, as we understand it, Article 82(5) enables a controller who has paid compensation in full to a data subject, in accordance with Article 82(4), to claim back part of the compensation from another controller who was involved in the processing in question and was partly responsible for the data subject's damage.

(C) The ICO may wish to emphasise in the code that a data sharing agreement which clearly sets out the controllers' respective areas of responsibility will help give effect to Article 82(5) by making it easier for one controller to recover from the other a proportion of the compensation paid out to data subjects.

(D) In addition, there is some uncertainty as to how Article 82 interacts with limits on liability agreed between parties in a data sharing agreement, with most people taking the view that the contractual limitations (such as liability caps) would restrict what could be claimed under Article 82. It would be helpful if the ICO could comment on what it considers to be the impact of such provisions in a data sharing agreement on claims against another controller under Article 82.

2.6 Ethics

We can fully understand the ICO's rationale behind the code's references to ethical considerations given the relationship between data protection principles and individuals' fundamental rights, as well as the principle of fairness outlined in Article 5. However, for clarity, the ICO may consider ensuring that such references (for example, on p. 86) refer explicitly to the fairness requirements of the GDPR. There may otherwise be a potential risk that they add an additional layer of obligation on controllers and increase uncertainty for organisations, as determining whether it is "right to share" or the "action of a responsible organisation" will be a subjective decision in many scenarios. It may therefore be helpful if the section on "Data ethics" was renamed "Fairness".

2.7 Examples

(A) We are very pleased to see that the ICO have provided a number of example scenarios in this draft and we would welcome more examples in the code. In particular, we would find more private sector examples useful as some chapters currently only contain public sector scenarios.

(B) In our view, it would be very helpful if the Annex E case studies included more commercial examples.

(C) On p. 104 of Annex E, two of the examples potentially could be replaced:

(i) the second example, "Public sector bodies sharing data to provide a co-ordinated approach", is very similar to the examples on p. 14 and 15 of the code, so a different example would perhaps be more useful; and

(ii) the third example, "Data sharing under the Digital Economy Act 2017", describes a scenario where only very limited personal data will be exchanged (such as the name of the director signing-off the accounts) so another example would, again, perhaps be more useful.

(D) We have drafted a list of potential examples for inclusion in the code at Annex 1. We would be happy to work with the ICO to further develop these or other examples.

3. Specific comments

3.1 Summary (p. 4 – 6)

(A) The bullet point at the bottom of p. 4 states that controllers must "identify at least one lawful basis for sharing data". As currently drafted, there is a possibility that it could be interpreted as permitting the selection of more than one legal basis. We understand from the ICO's guidance on "Lawful basis for processing" in the Guide to the GDPR that controllers need to identify the single most appropriate legal basis and not switch: "Take care to get it right first time - you should not swap to a different lawful basis at a later date without good reason. In particular, you cannot usually swap from consent to a different basis." The ICO may therefore wish to rephrase this bullet point and the same point which arises again on p. 37. Alternatively, if the ICO is referring here to the additional lawful basis that will need to be identified in relation to special category data, this could be made more explicit.

3.2 About this code? (p. 7 – 15)

(A) The code refers to data sharing needing to be "proportionate" at the top of p. 12. It is not clear how the requirement of proportionality interacts with the "necessity" test under the legitimate interests legal basis and the data minimisation principle, or whether the ICO views this as being part of the fairness concept. It would therefore be helpful if the ICO could clarify this.

(B) The ICO may wish to consider including the Article 6 legal basis for processing being relied upon for the data sharing in each of the examples on p. 14 – 15, as

this may make the examples more useful. As special category data is being processed in each of the examples, the ICO could also include reference to the Article 9 basis being relied upon, which is likely to be one of the health and social care grounds under Article 9(2)(h) and s. 10 and Schedule 1 DPA 2018.

3.3 Data sharing covered by this code (p. 16 – 19)

(A) The ICO may wish to amend the reference on p. 16 to the code not including "sharing data with employees or with processors" to cover workers rather than simply employees, to ensure that the broader pool of non-employee workers are also excluded if that is the ICO's intention. It would be helpful if this section also included some wording explaining the requirements for data sharing with employees/workers.

(B) The ICO may also wish to consider adding some additional wording to this section, perhaps by cross-reference to another piece of guidance, to address the position of independent contractors under the GDPR, for example, to clarify whether contractors should be viewed as:

(i) akin to employees and required to comply with the controller's data protection and IT security policies; or

(ii) processors in their own right, requiring processing terms in their service contracts.

3.4 Deciding to share data (p. 20 – 24)

(A) We agree with the ICO that DPIAs can be a very useful way for organisations to demonstrate their compliance with the GDPR, even where they are non-mandatory under the legislation and we welcome the guidance from the ICO on DPIAs in this section. However, we have a few suggestions below as to how the ICO may wish to amend the drafting of the code to clarify the ICO's position on non-mandatory DPIAs.

(B) On p. 21 the code states "You should regard it as good practice to do a DPIA". This wording seems rather unclear as to whether controllers have a real choice whether to carry out a DPIA or not. This position does not obviously fit in with that put forward in the ICO's list of scenarios that require a DPIA (as endorsed by the EDPB).

(C) In order to address these concerns we would welcome further clarification in the code in relation to there being no absolute obligation on controllers to carry out DPIAs (to the extent not mandatory under the GDPR). This clarification could note that controllers must be able to demonstrate compliance with data protection law and DPIAs are one way of doing so, but that they are not the only way. We think the wording in the "At a glance" introduction to this section ("We recommend you consider following a DPIA process…") is clearer and so we suggest that the ICO consider adopting this phrasing throughout the code, where this point arises.

(D) It would also be useful if the code expanded on:

(i) how DPIAs can be used as a "flexible and scalable tool" (as mentioned on p. 21), and how they can be "scaled down" for lower risk projects;

(ii) how controllers can demonstrate compliance with the code in relation to non-high risk projects by undertaking and documenting an analysis as to whether a DPIA is required, rather than by necessarily undertaking a DPIA in full; and

(iii) the extent to which a controller should consider carrying out due diligence on other controllers it wishes to share data with and the considerations controllers could take into account when carrying out such due diligence.

(E) The ICO may wish to expand the list of factors that should be considered by controllers in deciding whether to share data (on p. 21 – 23) to include:

(i) what the legal basis for processing is;

(ii) data minimisation considerations, such as what data is relevant and necessary to share and what data can be excluded from the sharing; and

(iii) transparency considerations, such as whether the current privacy notice provided to data subjects covers the anticipated data sharing or whether data subjects will need to be provided with an updated privacy notice and which entity will need to provide such notice.

We consider these points to be key considerations at the outset of a potential data sharing.

3.5 Data sharing agreements (p. 25 – 30)

(A) In the "In more detail" paragraph on p. 25, the ICO may wish to add a sentence acknowledging that data sharing provisions could be included as part of a larger agreement between the parties and do not need to be in a standalone data sharing agreement. For instance, data sharing provisions often appear in a business's standard terms and conditions.

(B) In relation to the "What should we include in a data sharing agreement?" section (p. 26 – 28), it may be useful for the ICO to include an acknowledgement at the start of the section explaining that the following list of points are included for consideration by data controllers, and may or may not be relevant depending on the nature of the data sharing in question.

(C) We do not consider that the data sharing agreement as the most appropriate place to document the analysis behind the data sharing – the agreement's purpose being to document the contractual relationship between the parties. Whilst the analysis will certainly influence the provisions of the agreement, we

consider that the analysis itself would be better housed in other GDPR documentation, such as LIAs, DPIAs or processing records (as appropriate). The ICO may therefore wish to consider removing the following from the "Data sharing agreements" section:

(i) the analysis as to why the data sharing is necessary, as suggested in the "What is the purpose of the data sharing initiative?" paragraph on p. 26;

(ii) the explanation of the anticipated benefits of the data sharing to individuals or society more widely, as suggested in the "What is the purpose of the data sharing initiative?" paragraph on p. 26;

(iii) the detailed analysis on the types of information to be shared and omitted from sharing, as suggested in the section on "What data items are we going to share?" at the top of p. 27;

(iv) the analysis as to the legal basis for processing, as suggested in the section on "What is our lawful basis for sharing?" on p. 27; and

(v) the conditions for processing special category or criminal conviction data under the GDPR and DPA 18, suggested in the section on "Is there any special category data or sensitive data?" on p. 27.

(D) In the "Which other organisations will be involved in the data sharing?" paragraph on p. 26, it would be helpful if the code clarified why the contact details for every organisation's DPO and key staff members need to be included in the agreement, as this requirement goes beyond the GDPR and it is not clear why the inclusion of this personal data in the agreement is necessary.

(E) Also in that paragraph, it may be useful if the code included an acknowledgement that a procedure for adding/removing organisations from the data sharing agreement is only required if the nature of the arrangement means that parties could join or leave.

(F) In the "Are we sharing data along with another controller?" paragraph on p. 26, it would be very helpful if the ICO could clarify the difference (if any) between what it considers should be in an agreement between joint controllers and that between independent controllers. There is a brief reference in that paragraph to joint controllers and their legal obligation to have an "arrangement" but other than that, the code does not differentiate. For example, Article 26 requires that an arrangement sets out the parties' respective responsibilities for GDPR compliance; but, based on the code, this is effectively what is required of all controller-to-controller data sharing, whether or not Article 26 applies. In addition, parts of the draft code appear to imply that data sharing renders the participants joint controllers. For example, on p. 52, the last bullet point 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 would therefore welcome more guidance on joint

controllers in the code, particularly in light of recent EU law decisions, such as the Fashion ID case.

(G) The ICO may wish to bolster the "What is our lawful basis for sharing?" paragraph to recommend that the parties agree who is responsible for obtaining the consent.

(H) The final sentence on p. 27, "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", could potentially be rephrased to make it clearer that responsibility for complying with access requests is not being allocated from the organisation to one individual, but that it should be clear as between the parties how such a request will be handled.

(I) In the "What information governance arrangements should we have?" paragraph on p. 28, there are two references to organisations in the data sharing having "common" arrangements. The ICO may want to consider rewording these references on the basis that it is unrealistic to expect parties in a data sharing to have "common" or the same arrangements in relation to data retention or security arrangements. Reference could be made instead to the parties all having arrangements that meet certain agreed standards.

(J) The penultimate bullet point on p. 28 ("have a timescale for assessing the ongoing effectiveness of the data sharing initiative and the agreement that governs it") seems to imply that the arrangement involves routine ongoing data sharing, the code should acknowledge that not all data sharing will be ongoing over a significant period of time.

(K) In the paragraph on "What further details should we include?" on p. 28 – 29, the ICO may wish to consider removing reference to:

(i) the suggestion for a summary of the key legislative provisions, as these could be replaced by cross-references; and

(ii) the suggestion for a diagram showing how to decide whether data is shared, as this could be a useful standalone resource rather than forming part of the agreement.

3.6 Accountability (p. 32 – 36)

(A) At the top of p. 33 there is a recommendation that, as part of being able to demonstrate GDPR compliance, where proportionate, controllers "must put in place a data protection policy, adopting a "data protection by design and default" approach". Further clarification on what is being proposed in terms of the content of the envisaged policy and when it would be proportionate for such policy to be put in place would be very useful. The ICO may also wish to consider removing the reference to "data protection by design and default" from this paragraph, on the basis that it otherwise needs substantial explanation.

(B) In the paragraph on "What documentation do we need to keep" (at the top of p. 34), the reference to only "larger organisations" being required to maintain records of processing activities should be amended as the current wording does not fully reflect the Article 30 requirements: smaller organisations which carry out certain types of (higher risk) processing are also required to maintain such processing records.

(C) In the next section, "What is the role of the Data Protection Officer (DPO) in a data sharing arrangement?" on p. 34, the current drafting of the code could potentially be interpreted as placing too much responsibility on DPOs, beyond what is required of them under the GDPR. It states "the DPO advises everyone on information governance [and] ensures compliance with the law", whereas Article 39 only requires DPOs to "inform", "advise" and "monitor compliance" with the GDPR. The ICO may consider rephrasing this section for clarity.

3.7 Lawful basis for sharing personal data (p. 37 – 42)

Although we can see the ICO are maintaining a consistent approach with the drafting in its lawful basis for processing guidance, the ICO may wish to revisit the summarised wording for the GDPR processing grounds included on p. 38, as they could potentially be misleading. The summary of the consent ground, we think, particularly risks causing confusion due to the amount of important detail and content lost.

3.8 Fairness and transparency in data sharing (p. 42 – 45)

(A) The ICO may wish to consider providing a cross-reference to its existing guidance on fairness and transparency, such as its detailed guidance on "the right to be informed", in this section rather than providing further detailed guidance here.

(B) If the ICO choose to continue providing detailed guidance in this section, the guidance provided should closely track the GDPR and clearly flag where the guidance departs from the GDPR. In particular:

(i) in the paragraph "How do we comply with the transparency requirements when sharing data?" on p. 44, the wording of the code appears to suggest that individuals are provided with the names of organisations' which share and have access to their data. This seems to cut across the option in the GDPR, as reflected on p.37 of the Article 29 Working Party guidelines on transparency ("WP260"), for controllers to provide information on the "categories of recipients" with which they share data; and

(ii) on p. 45, in the paragraph "What privacy information do we need to provide under the GDPR?", it is stated that controllers must "give the information directly to individuals". As Article 13 and 14 only state that controllers must "provide data subjects with the following information…" clarification on the requirement for the information to be provided "directly" to individuals would therefore be useful.

(C) We note that, in the case study on p. 100, there is a suggestion that the public sector bodies will fulfil the transparency requirement by updating the privacy notices on their websites, "as well as in correspondence and conversations". We would welcome clarification on whether this means:

(i) that the organisations in question would not have to write to everyone immediately, but only inform data subjects as and when they need to send them a letter; or

(ii) that updating the website is just one step so the organisations would need to pro-actively write to data subjects as well.

The ICO may consider amending this case study to more closely reflect the provisions of WP260, particularly in relation to changes to transparency information and the timing of notification of such changes (see p. 16 and 17 of WP260). For example, WP260 indicates that an enlargement of the categories of recipients of data will amount to a fundamental change in the data processing which should be notified to individuals well in advance of the change, which is not clearly reflected in the case study.

A private sector example would also be useful here to illustrate whether the ICO's view would alter with a commercial context.

3.9 Security (p. 46 – 49)

(A) In relation to data security, the current draft code seems to suggest, on p. 48, that a disclosing controller should be required to regularly audit the security position of the receiving controller. However, this would potentially seem to be hugely burdensome (administratively and financially) for a controller to have to continually monitor all third party controllers to whom it discloses data, despite the fact that those third party controllers have their own security obligations, and the data subject has a right of action against them. It also potentially suggests a greater level of responsibility than that for auditing processors. We suggest that this requirement therefore be reduced to refer to appropriate due diligence before the data sharing and to include audit rights in the agreement, where appropriate to do so.

(B) The code emphasises the importance of a compliance culture, and requires a disclosing controller to ascertain that the staff "across organisations [they] are sharing data with" understand the importance of protecting personal data (see p. 47). However, it is unclear from the current draft of the code how this exercise should be carried out in practice. The ICO may wish to review the drafting of this section to clarify that audits are not envisaged, as these will not be feasible for controllers in a weak bargaining position. Reference could be made instead to the inclusion of warranties in the data sharing agreement that address staff training.

(C) An "information risk analysis" is referred to on p. 48. It would be useful if this was defined and if the code could provide further explanation in terms of how this analysis interacts with DPIAs.

3.10 The rights of individuals (p. 50 – 56)

The code references individual complaints as being an "invaluable resource" (on p. 53). This does not seem to acknowledge that some complaints may not be well-founded. The drafting of this section should therefore recognise that controllers will need to evaluate and record (as part of their complaint handling process) whether the complaint is well-founded.

3.11 Other legal requirements

(A) It would be helpful if the section on "Do we have a legal power to share data?" on p. 58 was expanded to clarify how it applies to private sector organisations.

(B) In the section "Have you checked whether there are any legal prohibitions on data sharing?" on p. 61, it would be useful if examples were included of the "legal constraints on the disclosure of personal data, other than data protection legislation" that apply in private sector contexts.

3.12 Due diligence when sharing data following mergers and acquisitions (p. 70 – 72)

(A) The ICO may want to consider changing the focus of this section to cover commercial transactions more broadly, rather than focussing just on mergers and acquisitions. It could then address, for example, outsourcing, joint ventures, projects and strategic partnerships, as well as M&A. The points made in this section could then potentially be kept generic. Alternatively, if a focus on M&A is preferred, we suggest that this section be amended to reflect how M&A works in a more granular way. For example, there are a number of different stages during a merger or acquisition, and each of these raise slightly different issues in terms of data sharing considerations. As mentioned in the introduction to this submission, if it would be useful for the ICO to discuss this or any other aspect of the code in more detail, one or more representatives of the Committee would be very happy to meet with the ICO.

(B) The takeover example on p. 70 needs clarification. A takeover would be an acquisition of shares in a publicly listed entity, rather than the assets of another entity. We believe that the ICO are instead intending to refer to the acquisition of the business and assets of another controller: "For example, as part of a business sale, data might be sold as an asset to a different legal personality."

(C) To be as useful as possible, the ICO may wish to redraft the bullets at the top of p. 71 to make them more focussed on M&A, as they currently do not add substantially to the guidance in the previous sections. In particular:

(i) the first bullet point should be redrafted, as it currently does not reflect that some data will be transferred in the course of the due diligence process itself; and

(ii) the last bullet point should reflect that exemptions to the requirement to inform individuals may be available in this context, such as under Article 14(5)(b).

(D) We would welcome clarification on the meaning of the paragraph on "How do we manage shared data following a merger or restructure or other change of controller" on p. 71. If personal data passes from a seller to a purchaser on completion and a copy is not retained by the seller, we are not clear what "shared data" the ICO envisage there would be in such M&A context following completion of the deal. The example could refer to the purchaser integrating "seller data" rather than shared data.

3.13 Sharing personal data in databases and lists (p. 73 – 76)

(A) The ICO may wish to reconsider the "At a glance" section on p. 73 as some of the points seem duplicative: for example, the third and sixth bullet points. It would also be helpful if the list made clear that not all the points will apply to every situation, but that some will apply if data was obtained directly from data subjects by the proposed transferor, and others will apply if data was obtained by another party prior to its acquisition by the transferor. If the M&A section were widened to cover commercial transactions more broadly, this section could then be included or merged within it.

(B) The ICO may wish to amend the first sentence in the paragraph on "How does data sharing interact with direct marketing" on p. 75, in order to clarify its meaning, as it currently reads: "If this form of data sharing is relevant to your data sharing arrangement, you should read the ICO's detailed guidance on direct marketing". It possibly should read: "If this form of data sharing is relevant to your direct marketing arrangement, you should read the ICO's detailed guidance on direct marketing".

(C) In the section on "How does data sharing interact with political campaigning?" on p. 76, we consider that the paragraph on using a third party organisation to send out campaign materials is applicable to all marketing campaigns, not just political ones. Accordingly, we suggest that the ICO consider moving this paragraph to a more general part, such as the paragraph on "What else do we need to do?" on p. 75.

3.14 Enforcement of this code (p. 88 – 90)

In order to reduce the length of the code and ensure consistency with other evolving ICO guidance, the ICO may want to consider replacing this section with a cross-reference in the introductory section of the code to other ICO guidance on enforcement, including their latest regulatory action policy.

3.15 Annexes (p. 91 – 99)

We welcome the placeholder for data sharing checklists at Annex A (on p. 91), as we know that organisations find the ICO's checklists incredibly useful in practice. We are

sorry that draft checklists were not included at this stage and suggest that the ICO may wish to seek the input of practitioners on the checklists before the code is finalised.

If it would be helpful for the ICO to discuss with us any or all of these comments, then we would be happy to do so.

[redacted]

[redacted]

City of London Law Society

Annex 1

1. As a means of providing further clarification, the ICO may wish to include examples in relation to the following:

    (i) non-urgent data sharing between two parties in the context of a short term commercial project, such as the transfer of historic claims data from an insurer to an expert data analytics company in connection with the development of a new software system for handling insurance claims;

    (ii) data sharing in a commercial data pooling arrangement (as described on p. 18 – 19);

    (iii) data sharing that has a lawful basis, but is still considered unfair (as outlined on p. 43);

    (iv) commercial examples of when the disproportionate effort exemption to the transparency requirements (in Article 14) can be relied upon in a data sharing context (as referenced on p. 44);

    (v) data sharing in the context of a data trust (as discussed on p. 85); and

    (vi) data sharing in a regulatory investigation, where a regulator requests information from an organisation as part of their enquiries (see example below).

2. We would welcome the inclusion of more commercial examples in the code, these could include the following:

    (i) a financial institution sharing the personal data in a section of its mortgage loan portfolio with another financial institution, in the course of the sale of part of its mortgage lending business;

    (ii) a technology business sharing personal data of its customers and employees with another technology business, as part of an agreement between the two to share certain hardware and network functionality;

    (iii) a retailer sharing customer data with an expert customer support company, to enable the customer support company to provide a helpline service on behalf of the retailer;

    (iv) an online holiday booking portal sharing the personal data of holiday makers with individual holiday cottage owners;

    (v) two life science companies sharing personal data as part of a collaboration on a clinical trial;

(vi) a private sector organisation sharing data with lawyers or other professional advisers, in connection with legal claims;

(vii) a bank sharing data, relating to its staff, with a financial (overseas) regulator (who regulates that business); or

(viii) a private gym chain sharing the personal data of gym users with an insurance company, as part of a deal enabling gym users to receive reduced health insurance rates.