EMPLOYMENT
LAWYERS
ASSOCIATION

P.O. BOX 353
UXBRIDGE UB10 0UN
TELEPHONE/FAX 01895 256972
E-MAIL ela@elaweb.org.uk
WEBSITE www.elaweb.org.uk

Information Commissioner's Office consultation on draft Data Sharing Code of Practice

Response from the Employment Lawyers Association

5 JANUARY 2011

Data Sharing Code of Practice

Response from the Employment Lawyers Association

5 January 2011

INTRODUCTION

The Employment Lawyers Association ("ELA") is a non-political group of specialists in the field of employment law and includes those who represent both Applicants and Respondents in the Courts and Employment Tribunals. It is not ELA's role to comment on the political merits or otherwise of proposed guidance, rather to make observations from a legal standpoint.

ELA's Legislative & Policy Committee is made up of both Barristers and Solicitors who meet regularly for a number of purposes including to consider and respond to proposed new legislation.

A working party was set up by ELA's Legislative & Policy Committee under the chairmanship of Ellen Temperton of Lewis Silkin LLP to respond to the Data Sharing Code of Practice Consultation Paper (the "Consultation Paper"). Its comments are set out below. A full list of the members of the working party is annexed to the report.

ELA wanted to respond to the Consultation Paper because the Data Sharing Code (the "Code") does not fully or clearly address the common practical issues which employers face when sharing their employees' personal data.

The Committee has the following general comments about the Code before turning to the questions raised by the ICO in the Consultation Paper.

GENERAL COMMENTS

As a proposed source of guidance for employers handling their employees' personal data the Code's specific application to the workplace is far from clear. To support employers, or employees who need information about how their employers should behave, a clearer explanation of *how* the Code is relevant to the workplace would be appreciated. For the Code to operate effectively as guidance to employers specific examples of common workplace scenarios should be given. As there are existing sources of guidance for employers, most notably the Employment Practices Code, the introduction of a further source of overlapping guidance creates the potential for confusion, rather than clarity. It

would be better therefore to supplement the Employment Practices Code to address the purposes behind the draft Data Sharing Code and to direct employers to it, exempting employers from the need to have regard to this code as well.

This proposed code is apparently to be afforded the status of a Statutory Code of Practice. As such it creates an overlay of additional regulation with worrying consequences for employers if the Code does not provide clear guidance concerning its applicability. The proposed code also adopts an inconsistent approach to whether the reader is guided to other sources of guidance in relation to specific sections. As a general rule the working party feels that the reader should always be referred to existing guidance as it is often fuller and contains more specific guidance. The temptation to paraphrase them should be resisted as this can create the potential for confusion. However thought needs to be given to the effect of incorporating them into something which has the status of a statutory code if the underlying guidance does not.

The Working Party is concerned that "regulation" represented by this new Code is not permissive and sensible in tone. It appears primarily designed for public sector organisations and the advice to private sector organisations is inconsistent and wrong in parts. Contrast, for example, page 7, which states that "*Before disclosing or sharing information held by a private sector organisation you must also be able to identify a power which permits the organisation to do so. A private sector organisation's powers are likely to be set out in or to derive from its constitutional documents";* and page 31*, which states that, "If you are a private or third sector organisation then you may not need a specific legal basis for disclosing personal data but your protocol should still explain how the disclosures will be consistent with the DPA".* In addition to causing confusion, the page 7 advice is misconceived and suggests a fundamental misunderstanding of corporate constitutional documentation, to which most employees will have no ready access. The ICO should be giving advice only on the DPA, as it does more accurately on page 31.

To ensure that the new Code is not duplicative, burdensome and misleading for employers (particularly in the private sector) ELA would therefore recommend that ICO should either (1) amend the Data Sharing Code to make its application to the workplace clear and accurate; or (2) exclude the workplace from its scope and amend the Employment Practices Code and other relevant sources of guidance to bring them up to date and cover off any points from this Data Sharing Code which would otherwise be missed.

GENERAL

1. Does the code strike the right balance between recognising the benefits of sharing personal data and the need to protect it?

   Please see our comments above about the potential for the code to cause confusion and mislead employers and our comments on specific sections below.

2. Do we explain the legal requirements relating to public, private and third sector data sharing clearly enough?

   Please see our comments above and below.

3. Does the Code cover the different types of data sharing adequately, eg systematic, routine sharing or exceptional, ad-hoc requests?

   It is the working party's view that if the Data Sharing Code is to provide practical guidance to employers then the application of the Code to the workplace needs to be made a lot clearer, preferably by way of specific relevant examples.

   The practical difference between adhoc and systematic sharing in terms of compliance is not clear. In the employment context the concept of data sharing as defined in this draft code can cover a whole range of activities from systematic sharing in the context of in-sourcing and outsourcing, franchise arrangements (for example where an employer shares training records for the purpose of product training), and intra-group HR databases, to the more ad hoc, such as a one off request for information about an employee from a third party such as a regulator, or data flows in the course of due diligence exercises for corporate transactions which may or may not proceed, to data which is shared in the context of employment related litigation.

   One solution – as suggested above- would be to indicate that specific guidance is available in relation to the special category of the employment relationship and the unique volume and complexity of the issues surrounding employee personal data. This guidance would take the form of the Employment Practices Code. The Code should give serious consideration to amending the Employment Practices Code to include practical examples and guidance.

4. Is the code easy to understand? If not, how could we make it clearer?

   There is potential for confusion. Please see above.

5. Would the code benefit from a diagram or series of diagrams to illustrate various decision making processes? If so, which ones?

   No comment.

6. Is the code relevant to the types of data sharing your organisation is involved in? If not, which additional areas should we cover?

   See above: The Code does not adequately address the employment context.

7. Does the code deal adequately with situations where data is shared as a result of a merger or acquisition or through other organisational change?

As stated above this is an area where specific guidance to employees would be valuable. The Employment Practices Code is a valuable source of guidance for employers and employees alike and already addresses this issue although fuller guidance on this topic would be welcomed. It would be preferable to build on this existing guidance therefore, in the Employment Practices Code, as stated above. A link could be provided in the Data Sharing Code to the fuller guidance available to employers specifically to address the workplace.

8. Do we cover a broad enough range of examples? If not, could you suggest any other issues or scenarios that you think we should include.

   If the ICO decides not to exclude employment from this Data Sharing Code many more employment specific examples should be given. See our comments below in relation to the case studies.

9. Are the ICO's powers and penalties, and their relevance to data sharing, explained clearly enough?

   See below.

10. Is there anything else you think the code should cover or are there any other ways in which you think the code could be improved?

    Please see our general comments above and specific comments on each section below.

COMMENTS ON PARTICULAR SECTIONS OF THE PROPOSED CODE

SECTIONS 1 -3 PLEASE SEE OUR GENERAL COMMENTS ABOVE.

Section 4: Data Sharing and the Law

The working party refers to the General Comments set out above. The advice provided on data sharing and the law is problematic and as noted, suggests a fundamental misunderstanding of corporate constitutional documentation.

The working party considers that the ICO should focus on providing guidance on DPA issues. While there are of course other legal implications of sharing data in the public and private sector, the ICO's attempt to distil complicated legal issues within the Code in a discursive manner, is misleading, creates the potential for confusion, and as such, could prove to be counterproductive. A specific example of the potential for confusion from the guidance on page 7 of the proposed code is provided in our general comments above.

The working party suggests this section be revised and simplified to make reference to the relevant legal issues and the sources of guidance.. The Code could for example make reference to a requirement that any organisation considering data sharing must ensure it complies with the provisions of the DPA, which implements the EU Directive and refer to the potential relevance of other professional guidance, voluntary industry codes but also other laws and legislation which may include: the tort of breach of confidence the European Convention on Human Rights (ECHR), the Human Rights Act 1998 and the Freedom of Information Act 2000.

Section 5: Deciding to Share Personal Data

The working party takes the view that this section does not provide adequate practical guidance, particularly regarding the application of the Code to the workplace. We suggest that this section is revised to indicate that specific guidance is available in relation to the special category of employee personal data in the form of the Employment Practices Code and then to amend that Code to include practical examples and guidance.

Section 6: Fairness, Transparency and Consent

The working party's comments on section 6 of the Data Sharing Code broadly mirror the General Comments set out above: the guidance provided in the Code on the issues of

fairness, transparency and consent does not take account of the particularities of the employment context and, accordingly, is unlikely to prove of any real assistance to employers who wish to understand the nature of their obligations when sharing personal data.

For example, the section of the Data Sharing Code on “Privacy notices” does not address when and how employers should inform job applicants and employees about how their data will be shared. Generally speaking, employers address this obligation in the context of a broader policy document issued to all employees, and the lack of any specific reference to how this present draft guidance works in the employment context is likely to leave employers confused.

Similarly, the commentary in section 6 of the Data Sharing Code on “Consent” does not take account of the ICO’s separate guidance for employers on the difficulties of obtaining valid consent in the employment context and the ICO’s general recommendation that employers rely upon other conditions to legitimise their processing of personal data. Again, employers who refer to this section of the Data Sharing Code may be left confused as to whether they can rely on consent to legitimise data sharing.

In light of these points, the working party considers that section 6 of the Data Sharing Code should be revised to include specific guidance and examples relating to the employment context, or alternatively as we have requested above, employment should be excluded from this Code and addressed in an updated version of the Employment Practices Code.

Section 7: Security

The comments which the working party has made in relation to other sections of the proposed code apply equally to this section in that there are already a number of sources of guidance on a data controller should meet its obligations under the DPA to have adequate and appropriate technical and organisational measures in place. As a general principle it is desirable to have all this guidance in one place. This section of the proposed code should therefore explore how these existing sources of guidance are specifically applicable to situations where data is shared whether on an ad hoc or more continual basis. The reader should expressly be referred to those sources of guidance and to avoid potential for confusion the temptation to paraphrase them should be resisted.

Although the guidance contained in this section is helpful it is incomplete which is another reason for directing the reader to fuller sources of guidance.

More clarity would also be desirable in relation to specific words and expressions; how for example is the reader to assess whether information is "valuable" as whether it is so depends on its value to the recipient (whether the intended recipient or otherwise) or the data subject and the data controller is not always in a position to judge this. In its guidance on monetary penalties the ICO has referred to information being sensitive both in the DPA sense and in the sense of its importance such that financial information, although not defined sensitive personal data under the DPA is nonetheless regarded as sensitive by the data subject in terms of the potential for harm if it falls into the wrong harm. To introduce a further concept of "valuable" is not necessarily helpful whereas the ICO's explanation of what is sensitive in its guidance on monetary penalties is perfectly workable.

The proposed code goes on to say that the data controller should aim to build a culture of security awareness and good practice "*especially in respect of data received from another organisation".* In the working party's opinion data received from a third party should not be afforded a higher level of care than the data which the data controller holds on its own employees. The ICO should clarify what is meant by this expression.

The proposed guidance also suggests that the DC can meet its obligations by *"visiting premises periodically to check that security procedures are being adhered to..." .* The employer who shares data in the context of an insourcing or outsourcing or international transfer may not be in a position practically to follow this guidance and would benefit of the guidance would go on to provide examples of other ways in which they could comply with their obligations.

Section 8: Governance

Please see our comments below on the data sharing protocols.

While this section is generally helpful all the examples which are given in relation to data standards policies are public sector. The code should explain their application to private sector organisations and in particular to employers.

Under the section which deals with the review of data sharing arrangements the working party was concerned by the expression "information sharing must be necessary, proportionate *and have a positive outcome for individuals or for society more widely"* (our emphasis). The proposed code will be a statutory code and therefore much more guidance should be provided on how this will be tested. In many employment context the individual data subject may not agree that the outcome was necessarily a positive one for them as may

be the case where an employee who is seconded to another organisation is disciplined or performance managed. In any event the working party is dubious as to whether this is the correct test under the DPA, or indeed what the legal basis for this statement actually is. Reference may perhaps be made to DPA, Sched.2 para 6 (1) although it is submitted that this is not the same as saying that the outcome needs to be positive.

In this same section, the bullet points suggest that the DC should ensure that it is making it easy for the DS to access their shared personal data and requires the DC to respond to queries and complaints promptly. Examples of how this might work in the employment context should be given or the reader referred to relevant guidance on data subject access requests. The breadth of this comment could otherwise be criticised for ignoring the complexity and specific issues faced by employers when complying with DSARs made by employees. The guidance should specifically address how this applies to the atypical worker who may be insourced, outsourced or supplied by an agency.

Section 9: Individual's Rights

Please see our comments above in relation to atypical workforces.

This section ignores the complexities of complying with DSAR requests from employees due to the volume of relevant records which can be created (by for example email) and the period of time over which such employment records can be created. As many records may be contained in email it also ignores the issues which many employers face in having to reconstitute email and search archived tapes. What is the extent of the employer's obligations in this respect when the employee is for example seconded to another organisation and data is shared between them? The original employer should not be a DC in relation to the vast majority of email records on the host employer's system but suggesting that one request can be made by the data subject rather than multiple requests oversimplifies the issue. Specific guidance- rather than the broad statements here which gloss over the practical difficulties of compliance- should be given of how the rules apply to the data sharing context.

As is noted above therefore tailored guidance for the employment context would be desirable.

Section 10: The ICO's Powers and Penalties

This section is a summary of the ICO's powers and penalties. As such, the working party

found it to be quite limited, as it is neither a complete summary, nor a simple index for further research.

It is helpful to see a list of the options available to the ICO but this information (and more) is available on the ICO's website and in other guidance documents. If this section is retained it could be improved by the addition of examples for each of the options and further explanations. For instance, the notes on "Enforcement Notice(s)" end with the statement that "Failure to comply with an enforcement notice is a criminal offence" yet there is no further explanation of the prosecution of such an offence, nor the criminal sanctions. Having now issued increased monetary penalties (under the new regime), examples of the amounts of fines could be given in this section.

In terms of the audit options, the code notes that compulsory and consensual audits may be undertaken, although the focus is mainly on compulsory audits. There is no more information on what a consensual audit is, for example the application process and how it works in practice, which would be helpful here.

This section of the code contains several links to other documents, including the guidance on monetary penalties, the assessment notices code of practice and the Data Protection Regulatory Action Policy. These separate documents contain the relevant information on those specific aspects of the ICO's powers and penalties, so this section of the code really only acts as a marker to them and we wonder whether it adds anything as a result. As the links only work when viewing the document on-screen, a hard copy of the code will be less useful, as readers will need to access the links online. Therefore, users who have downloaded and printed a copy of the code will not have the complete code, unless they also print the additional documents, or refer to them separately

Section 11: Notification

This section of the code is really very limited. It seems to apply only to existing data controllers who need to ensure their notifications are up to date, to allow the sharing of personal data and therefore assumes that users of the code already understand the notification process and have completed it. Again this topic is covered expansively elsewhere and the working party questions what is gained by including it. The section also reminds organisations that are sharing personal data to be clear about the personal data each is responsible for and to include that information in their notification entries. In reality this can be difficult to assess and the statement seems to gloss over the practicalities,

without offering any advice.

For completeness, if this section is to be included, more information on notification should be included in this section of the code and as drafted, it is rather 'back to front'. It ends with a link to "find out whether you need to notify under the DPA" (although at the time of writing this response, the link was not working), whereas users should already have notified with the ICO; if not, then this section definitely needs to be fuller and contain the links to notification at the start.

Section 13: Things to Avoid

The bullet points list various "things to avoid" when sharing personal data, which essentially mirror some of the data protection principles. For example, not "sharing excessive or irrelevant information" and not "having inappropriate security measures in place".

These are generally common sense points, mostly illustrated by examples, but given that the code makes it clear that such practices "could lead to regulatory action" it is insufficient to make a simple statement that you should avoid "using incompatible information systems to share personal data, resulting in the loss, corruption or degradation of the data", without explaining this further.

As this section is so clearly focused on the data protection principles (albeit oddly reversed as what "not" to do), it might be better to simply list all 8 of the data protection principles, reminding users what they are and including these bullet points under each, as appropriate.

Section 14: Suggested Contents of a Data Sharing Protocol

This section suggests that where different organisations decide to share information in a specific initiative, a specific legal document should be drawn up providing “essentially a set of common rules binding on all the organisations involved”. No examples are given of suitable initiatives for the drawing up of such a protocol in this section, however. It is notable that the following section, 15 (case studies), while providing examples of particular data sharing initiatives does not itself follow the data sharing protocol idea through.

The protocol suggested is plainly envisaged to be quite a complex document and would benefit therefore from the inclusion of examples in section 14. (see the detailed information it is suggested should be included under the heading “Information Governance” on page 31 and the lists of suggested appendices on page 32.) It would be useful to understand when

the ICO genuinely believes would justify this amount of administrative work, particularly when it only leads to a document which the Data Sharing Code admits "does not provide any form of legal indemnity from action under the DPA or other law".

In the employment context, the initiatives most likely to justify work on this scale might include the installation of a group-wide database of employee information, or perhaps a very large-scale disposal or acquisition of businesses where data is being shared with a number of corporate purchasers. But if this is the sort of initiative intended, the Data Sharing Code gives strangely acontextual and uncommercial advice. In the former case, for example, particularly where the group includes entities outside the EEA (or the server is outside the EEA), most sophisticated employers would already have other documentation in place to deal with cross-border transfers. It would be more sensible for the employer to incorporate some of the ideas set out here in the existing documentation. Where corporate transactions are involved, most organisations are likely already to have a commercial contract and confidentiality agreements in place. It is therefore questionable whether a separate protocol is actually necessary. By giving very broad advice which does not recognise context, the Data Sharing Code risks being seen as unhelpful and duplicative.

The Employment Practices Code already deals with many of the issues covered by the protocol section: see, for example, the explanation of what to do when an organisation receives a DPA or FOIA request (covered in the section 2.10 entitled "Disclosure requests" of the Employment Practices Code), as well as the existing sections at 2.10 on Disclosure Requests and 2.11 on Publication and other Disclosures. The section on data sharing protocols adds little to this save a reminder that record-keeping about when information is shared some of the suggestions teach people how to store information efficiently (dates of birth in common format, for example) but do not go on to provide guidance on how to do so fairly and lawfully.

Section 15: Case Studies

Only three of the case studies relate to employment (Retailer database of employees dismissed for stealing; anti-fraud exercise involving benefit fraud by public sector employees; anti-fraud exercise involving public sector employees moonlighting with other public sector employers). The latter two examples are already covered by section 2.7 of the Employment Practices Code (although there is a little new advice on deletion of data at the end of the exercises and the need to investigate complaints due to inaccurate data). As stated before, it would be better to amend the Employment Practices Code to include this additional advice.

The first example is highly specific in practice and the advice that the data involved can be used in this way questionable it involves the publication of sensitive data (the commission or alleged commission of the offence of stealing) without any ostensible guidance concerning the need for satisfaction of a Schedule 3 condition. (Condition 7A of Schedule 3 perhaps although it is far from clear that such a grouping of retailers would qualify as an “anti-fraud organisation” because it is unclear that sharing the names would prevent fraud). The standard for fair dismissal is not the same as the criminal standard of proof that any fraud actually occurred.

MEMBERS OF ELA WORKING PARTY

Ellen Temperton, Lewis Silkin LLP (Chair)

Ivor Adair, Russell Jones & Walker LLP
Daniel Aherne, Olswang LLP
Khurram Shamsee, Beachcroft LLP
Andrea Ward, Hogan Lovells LLP
Alison Wetherfield & Razia Begum, McDermott Will & Emery LLP

About you

Please use this section to tell us about yourself

Full name	
Job title or capacity in which you are responding to this consultation exercise (e.g. member of the public etc.)	
Date	5 January 2011
Company name/organisation (if applicable):	Employment Lawyers Association
Address	P.O. Box 353 Uxbridge
Postcode	UB10 0UN
If you would like us to acknowledge receipt of your response, please tick this box	☐ x (please tick box)
Address to which the acknowledgement should be sent, if different from above	lindseyw@elaweb.org.uk