28 February 2013

Our ref: ICAEW Rep 34/13

Your ref:

By email: consultations@ico.gsi.gov.uk

Dear Sirs

Subject Access Code of Practice

ICAEW is pleased to respond to your request for comments on *Subject Access Code of Practice*

Please contact me should you wish to discuss any of the points we raise. We would welcome an opportunity to make further representations or discuss our response.

Yours sincerely

Felicity Banks
Head of Business Law

T +44 (0)20 7920 8413
E felicity.banks@icaew.com

ICAEW REPRESENTATION

SUBJECT ACCESS CODE OF PRACTICE

Memorandum of comment submitted in February 2013 by ICAEW, in response to the Information Commissioners Office consultation paper *Subject Access Code of Practice* published in November 2012.

Contents **Paragraph**

INTRODUCTION

1. ICAEW welcomes the opportunity to comment on the consultation *Subject Access Code of Practice* published by the Information Commissioners Office on issued on 29 November 2012, a copy of which is available from this link.

2. We would be happy to discuss any aspect of our comments and to take part in further consultations on this area.

WHO WE ARE

3. ICAEW is a world-leading professional accountancy body. We operate under a Royal Charter, working in the public interest. ICAEW's regulation of its members, in particular its responsibilities in respect of auditors, is overseen by the UK Financial Reporting Council. We provide leadership and practical support to over 140,000 member chartered accountants in more than 160 countries, working with governments, regulators and industry in order to ensure that the highest standards are maintained.

4. ICAEW members operate across a wide range of areas in business, practice and the public sector. They provide financial expertise and guidance based on the highest professional, technical and ethical standards. They are trained to provide clarity and apply rigour, and so help create long-term sustainable economic value.

5. This response reflects consultation with the ICAEW Business Law Committee which includes representatives from public practice and the business community, and which is responsible for ICAEW policy on business law issues and related submissions to legislators, regulators and other external bodies. The response also reflects comments from members of ICAEW's Insolvency Committee and Data Protection Working Party. The response is made on behalf of members both in the context of public practice and as employers in the UK.

MAJOR POINTS

Support for the initiative and summary of views

6. ICAEW is supportive of the creation of a Code which consolidates the Information Commissioner's existing guidance. This is an area where members have sought advice from the ICAEW, raising a number of difficult issues, and where clearer guidance would assist our members in complying with their obligations The Code provides a useful start but we have a number of concerns, set out below. Where it is not possible to incorporate or respond to these, we would welcome separate discussion or engagement to resolve these concerns.

7. We recognise that subject access requests are an important part of the data protection regime in both the UK and the EU. Our members accept that individuals have a right to know what information is held about them and, when acting as data controllers, are legally required to comply with such requests under UK and European law. Nonetheless, ICAEW is aware of the burden and difficulties faced by members when complying with these requests.

8. In particular, we are concerned that the Code fails to adequately address the problems that arise from excessively broad subject access requests, particularly those involving unstructured electronic information. These concerns are described in further detail below. A failure to adequately address these issues in the Code is likely to result in an inconsistent approach to such rights and the continuing need for regulatory intervention by the Information Commissioner.

9. It would be useful if the Code addressed situations in which there are multiple data controller and data processor relationships. One example is insolvency situations. The Code ought to recognise that in a corporate insolvency, the insolvent company is a separate data controller to

the insolvency practitioner and that where the insolvent company has ceased to trade there will be real practical difficulties in it responding to a subject access request.

10. In personal bankruptcies the Code should reflect the fact that subject access requests are often used to challenge the process undertaken to realise the bankrupt's estate. This is particularly inefficient given the personal data disclosed is likely to be of little value. There are better courses of action available to the bankrupt wishing to question the actions of their trustee in bankruptcy. In both corporate and personal bankruptcies the Code should recognise the cost of responding to subject access requests will reduce the funds available to creditors and so have a direct and detrimental effect on others.

11. The Code should provide guidance and manage the expectations of both data controllers and individuals. There are a number of legal cases which limit or define the rights of individuals under subject access requests, but the draft Code does not appear to give any guidance to either data controllers or data subjects on these limitations. Some individuals appear to believe that a subject access right entitles them to the same disclosure as would be provided under the Civil Procedure Rules and/or access to any personal data held about them anywhere within an organisation no matter how impractical it is to locate that information in practice. These expectations are not realistic and result in significant dissatisfaction with the operation of the Data Protection Act 1998. It would be of assistance to all parties of this Code could address these expectations, as well as leading to a more consistent response to subject access requests.

Excessively broad requests - general

12. ICAEW acknowledges that even if a subject access request is drafted in very broad terms it is normally possible to discuss the matter with the individual to identify the personal data they are really interested in. However, in a some instances individuals refuse to narrow the scope of their search and still expect data controllers to search all or substantially all of their systems in order to identify personal data. For the reasons set out below, this sort of very broad request can be difficult, and in some cases impossible, to comply with.

13. Unreasonable requests are normally resolved by the data controller either refusing to conduct a search or unilaterally narrowing the search criteria used to identify personal data. So long as the data controller has taken reasonable steps to comply, we understand that the Information Commissioner has not generally sought to take further action even if the individual continues to insist on a complete search of all information held by the data controller. It is disappointing that this informal, though sensible, approach to dealing with excessively broad requests is not reflected in the guidance.

Excessively broad requests - structured v unstructured electronic data

14. Very broad subject access requests are particularly problematic when they extend to unstructured electronic information, such as emails, word documents and the like. The problems arise due to:

- **A lack of indexation**. Individuals might be referred to in a number of different ways. For example, an individual called Christopher Graham might be referred to in a number of ways, including 'Chris', 'Mr Graham', 'CG' and numerous other variants and nicknames. Moreover, not every reference to 'Chris' will be to 'Christopher Graham', they might well be to a completely different person. The only way to accurately identify personal data about a particular individual is to conduct a manual review, which even then might not always be accurate. The Code suggests that 'systems [should] have the technical capability to search for the information necessary to respond to a SAR, but they should also operate by reference to effective records management policies' (page 18). It is very unclear how this would apply to unstructured electronic data such as emails. Whilst it is relatively easy to conduct keyword searches for individual's names and variants of names it is unlikely this would be completely accurate and it would be very difficult, if not

technologically impossible, to implement a completely accurate automated alternative. The only possible way to do this might be oblige all users of emails to use a uniform naming convention (ie unique ID) whenever they refer to any individual in any document. However, this would be both impractical and unrealistic ;

- **Mixture of information**. With unstructured electronic data, there is little control over the information they contain. An email containing personal data about one individual might: (a) contain personal data about other individuals (either separate from or combined with the first individual's personal data); (b) contain information that is not anyone's personal data; or (c) be partly or wholly exempt from disclosure based on the exemptions set out in the Data Protection Act 1998. Again, the only way to extract relevant personal data, and apply appropriate exemptions, is to conduct a manual review. We do not think it would be possible to automate this process. Moreover the need for careful and diligent review is reflected by enforcement action by the Information Commissioner, such as the Undertakings sought from Royal Cornwall Hospitals NHS Trust following the inappropriate disclosure of third party sensitive personal data in response to a subject access request; and

- **The need to archive information**. The fact that unstructured electronic information is a mixture of many different types of information means that it is difficult to determine how long it is required to be kept. As a result it is often archived on a precautionary basis, particularly in light of legal or regulatory obligations. Including archived data within the scope of a subject access request can greatly increase the cost and difficulty of responding.

15. In summary, subject access requests can work well when applied to structured data which allows information about a particular individual to be quickly and easily located and extracted. The position is much more difficult for unstructured electronic information which will almost always have to be searched manually in order to locate and extract relevant personal data.

16. It is important to note that this does not just relate to the cost and difficultly of responding to a subject access request. It also relates to the relevance of that personal data to the individual. Where information is inaccessible and hard to locate it is highly unlikely it would be used in a way that would impact on that individual's privacy , so it is hard to see why there is a strong entitlement to access that information. It is suggested that such information is not personal data as it has ceased to relate to that individual in any meaningful way.

Excessively broad requests - practical considerations when searching

17. Very broad requests are also problematic due to the sheer volume of information now held by many organisations. A large organisation might well have tens of thousands employees and over a billion emails. It will also hold other unstructured electronic information such as word documents, spreadsheets, instant messages, SMS texts and the like. This information might be held in multiple different systems and therefore may need to be extracted in different ways.

18. It is simply unrealistic to expect an organisation to search all of this information in response to a subject access request. The unstructured nature of this information means that it is impossible to accurately identify information about an individual and, instead, it is necessary to use more inexact methods such as key word searching followed by a manual review to further filter that information.

19. To take the example given above, an individual with a common name, such as 'Christopher Graham', makes a subject access request an organisation with perhaps 100 million emails. Automated keyword searches for 'Chris', 'Christopher' and 'Graham' could be used reduce the number of emails requiring further review by, say a factor of 1000 (though this filtering exercise would itself be a very expensive and time consuming undertaking). This would still leave 100,000 emails to review. Let us further assume that it takes, on average, 5 minutes to review, apply exemptions and extract relevant personal data from each email. This would still mean it

would take over 1,000 working days in order to process that information to respond to a request.

20. No organisation could be expected to go to these lengths to respond to a subject access request and the ICAEW's understanding is that this is not how subject access requests are dealt with in practice. Instead, data controllers facing this type of request will commonly unilaterally limit the scope of the search based on factors such as:

- keywords that are likely to identify the individual and the particular issue of concern;
- particular date ranges intended to reflect the period during which the individuals concerns have arisen; and
- particular custodians (eg email accounts) likely to hold relevant information.

Excessively broad requests - areas of practical difficulty

21. In addition to the general factors above, there are a number of specific issues that arise when responding to subject access requests:

- **'Own' information**. The subject access request may apply to information sent or received by, or 'cc'd' to, that individual. To what extent is the individual entitled to such information? For example, if an employee were to leave an organisation, would they be, prima facie, entitled to a complete copy of all emails in their mail box on the basis that it is 'their' personal data? Would it be necessary for the organisation to review and filter that account to remove information that it not that individual's personal data (on the basis of Durant v FSA) or is exempt (for example, because it contains personal data about another person)? How would the exemptions apply in a situation in which the individual has already seen and is aware of that information?

- **CCTV**. Subject access requests for CCTV can be problematic because it may be necessary to manually review CCTV footage in order to identify images of an individual, it is difficult to redact third party personal data and in some cases it can be difficult to confirm that the individual has been accurately identified. Should individuals seeking CCTV footage normally be expected to provide details of exactly where and when the footage was taken?

- **Other systems:** Organisations may have a range of systems recording personal information such as security badge access logs, time recording systems, cashless payment systems etc. To what extent are data controllers expected to search all such systems in response to a subject access request? Should a data controller only be expected to search these systems where specifically and reasonably asked to do so?

- **Public information:** Are organisations expected to search and provide public information in response to a subject access requests? For example, if the applicant making the request is a public figure, is an organisation expected to provide press cuttings and similar material about that individual just because such information is on its systems somewhere?

22. These are all difficult issues but ones that data controllers have to grapple with on a regular basis. We suggest that they should be addressed in the Code to ensure that data controllers' and individuals' expectations are better aligned and to avoid unnecessary intervention by the ICO.

Insolvency issues

23. Subject access requests can be problematic in corporate insolvency situations, not least because of the confusion over the status of the insolvency practitioner. They will generally be a separate data controller to an insolvent company with a relatively limited remit - that is to maximise returns for the creditors of the company, thus minimising the adverse economic and

social impact of its insolvency. The insolvency practitioner will not generally become involved in the detailed management of the company or its records, though it is required to ensure that its accounting and business records are secure. The insolvent company will remain data controller over its records and a subject access request for personal data in those records must be made to it.

24. There are a number of practical implications to this distinction. In particular, in many cases it may be difficult for the insolvent company to respond to a subject access request. It may have ceased to trade and no longer employ any staff to locate and extract the necessary information . Equally the insolvent company may have shut down its information technology systems. It would only be possible to respond to requests by first restoring those systems and then extracting the relevant personal data. This is likely to be extremely expensive if not impossible (for example, where those systems no longer work or are not supported).

25. Where the insolvency company is able to respond to a subject access request, it will incur costs in doing so. This will reduce the funds available to creditors of the insolvent company. Compliance with the subject access request will therefore have a direct and detrimental effect on third parties.

26. Finally, any personal data provided to the individual will be of limited value. Where the insolvency company has ceased to trade the personal data is effectively 'dead' and unlikely to be further used in a way that infringes that individual's privacy. In particular, once a company ceases to trade it is very unlikely that it would disclose the individual's personal data to a third party or use that personal data to make a decision about that individual. Even if the data does infringe the individual's privacy in some way, they will not have a meaningful remedy given that any action by the individual against the insolvent company is likely to be stayed or, even if successful, result in that individual becoming an unsecured creditor.

27. Subject access requests are slightly different in personal bankruptcies where the insolvency practitioner often takes over the debtor's financial records as part of his estate. Accordingly, the insolvency practitioner may be more likely to become a data controller over that information. The debtor may try to challenge the process undertaken to value and sell their property (for example, challenging the sale price for their house) using a range of tactics, including subject access requests. If the debtor's estate has insufficient assets to pay their creditors, as is commonly the case, the cost of responding to the subject access request will fall on the creditors. We question the appropriateness of subject access requests in these circumstances. The debtor loses nothing by making the request but is likely to get little or no benefit. Their real concern is the realisation of their assets which is better addressed through other routes such as a challenge to the conduct of the bankruptcy under sections 303 or 304 of the Insolvency Act 1986 or a complaint to the Insolvency Service or the insolvency practitioner's regulatory body. Moreover the personal data disclosed will be of little value as it is unlikely to include, for example, privileged material or correspondence between the insolvency practitioner and the creditors. However, the subject access request will cause real detriment to the creditors by reducing the funds available to them.

28. ICAEW is not suggesting that subject access rights should be disapplied in insolvency situations, but that the Code should recognise and give guidance on how these factors should be taken into account when assessing the level of effort necessary to respond to a subject access request. The Code should also recognise the status of an insolvent company as a separate data controller to the insolvency practitioner in a corporate insolvency.

The Legal Framework

29. It would be helpful if, amongst other things, the Code provided clearer guidance on how to deal with broad subject access requests and provided a better balance between the rights of the individual and the rights of the data controller and third parties. Such guidance would be compatible with both UK and European law and would result in more consistent responses to subject access requests than would result from application of the current draft Code.

30. From an English law perspective, the ability of a data controller to limit himself to a 'reasonable and proportionate' search was recognised by the courts in Ezsias v Welsh Ministers [2007] All ER (D) 65. Moreover, in Elliott v Lloyds TSB Bank Plc & Anor [2012] EW Misc 7 the court reiterated this position and specifically stated that the 'disproportionate effort' limitation in section 8(2) exempted data controllers from not only the obligation to provide copies of personal data but also the obligation to locate that data in the first place, the obligation to make searches being 'part and parcel' of the obligation to supply personal data.

31. The need to apply subject access rights in a proportionate manner is also reflected in European law, which makes clear that all Directives are subject to the principle of proportionality, as provided for in R (British American Tobacco Investments) v. Secretary of State for Health (C-491/01). In addition, the rights of the individual must be balanced against the rights of data controllers, including their freedom to conduct business under article 16 of the Charter of Fundamental Rights of the European Union. These include a right for business not to be subject to unnecessarily complicated or costly obligations (see SABAM v Netlog (C-360/10)).

Practical solutions

32. ICAEW suggests that the Code should provide clearer guidance on how to deal with broad subject access requests and that the guidance should better balance the interests of data controllers and individuals. ICAEW suggests that the level of effort required should be determined by reference to the following factors:

- The **value of the personal data** – ie the extent to which it is reasonably likely to infringe that individual's privacy or that the individual needs to check that his personal data is accurate and is processed lawfully (see recital 41 of the Directive). This is clearly the most important factor in determining the lengths to which a data controller should go to locate relevant personal data. On the one hand the scope of any search should include personal data that is likely to seriously affect the individual's personal integrity or is used in a manner likely to seriously affect that individual's privacy. On the other, there seems little purpose searching for personal data that has little impact on the individual's privacy (such as old or archived emails);

- The **presence of litigation** and the extent to which the information is available by other means. It is clear that an individual is entitled to make a subject access request before, during and after litigation (Durham County Council v Dunn [2012] EWCA Civ 1654). However, ICAEW suggests that the desire to obtain information for the purposes of litigation should be disregarded when assessing the value of the personal data to the individual (ie as that information ought to obtained through disclosure);

- **Archived electronic information** should be excluded save in exceptional circumstances. As discussed above, information is generally archived for legal and regulatory purposes and is only likely to be restored for those purposes. Where there is no intention by the data controller to restore that information to process a particular individual's personal data there should be no obligation to restore it in order to respond to a subject access request. Clearly there will be exceptions, for example where the information has been archived to keep a record about a particular individual or the personal data is of critical importance to the individual. However, given extracting archived data can be expensive, ICAEW considers that this would only be required infrequently;

- **Electronic data back ups** should also be excluded save in the most exceptional circumstances. The backed up data will generally also exist on a live system - the purpose of the back up being to replicate data from the live system. Where the data exists on a live system there seems no purpose recovering it from a back up (even if it might 'materially differ' from the live version, see page 27 of the Code) as the back up is only of historic

interest having no further relevance to the 'live data'. Alternatively, if the data no longer exists on the 'live' system that is likely to be because it has been deleted and therefore the back up ought to be treated as 'Deleted information' and not subject to a search (per page 27 of the Code). There may be exceptions but given the significant cost and expense of recovering back ups those exceptions would be very rare.

- The **resources available to the data controller**. Many of the ICAEW's members are small firms or sole practitioners and only have limited resources available to respond to subject access requests. Having to spend tens' or hundreds' of hours responding to subject access requests would be very burdensome for many of those members; and;

- **Insolvency**. The particular issues arising on insolvency (set out above) ought to also be addressed.

33. It would be useful to provide some practical examples of the steps a data controller might be expected to go to, to search for personal data. A particularly useful example would involve a subject access request from an ex-employee for copies of emails, and would set out the steps the data controller might reasonably take to respond to that request, including keywords relevant to the circumstances of the particular example, how many mailboxes should be searched and the likely date range over which the search should take place. Such an example would be especially useful to employers and insolvency practitioners.

34. Finally, it would be useful to provide a benchmark level of effort a data controller should expend in order to respond to a subject access request. This could, for example, be based on the level of effort necessary to respond to a freedom of information request, i.e. a maximum of 18 hours of effort to locate the relevant information. This benchmark figure could of course vary according to the circumstances set out above, so that if the personal data were critical to that individual's personal integrity greater effort would be needed. Conversely where the personal data is only likely to be of limited value to the individual, a lower limit might apply. ICAEW acknowledges that the decision in Elliott v Lloyds TSB Bank Plc & Anor [2012] EW Misc 7 could be read as requiring greater effort but it suggests that there was no clear decision in that case about the exact level of effort needed (the decision instead being made in response to the particular facts of that case) and that there were reasons why more effort was appropriate in that case compared to many other subject access requests.

35. This would be a significant change to the draft Code but believes that this framework would lead to a more consistent response by data controllers to subject access requests and would manage expectations amongst individuals. This would reduce the need for the Information Commissioner to work closely with data controllers when managing difficult subject access requests and allow valuable data protection resources to be used more efficiently elsewhere.

36. Finally, this revised approach would be consistent with the Government's stated desire to reduce red tape and ensure that existing regulation are implemented in a manner that does not impose unnecessary burdens on business (see The Cabinet Offices' Red Tape Challenge). The Code needs to be drafted in a way which does not impose unnecessary obligations on business, including by a failure to address ways in which decided cases have already lessened their obligations.

RESPONSES TO SPECIFIC QUESTIONS

Q1. Does the code adequately explain how the Data Protection Act 1998 (DPA) provides subject access rights for individuals?

Yes. Subject to the comments above on excessively broad subject access requests.

Q2. Does the code adequately explain what an organisation is required to do in order to comply with its legal obligation under the DPA to provide subject access?

Yes. However:

- this is subject to the comments above on broad subject access requests; and
- it would be helpful to have further guidance on what information should be provided under section 7(b)(i)-(iii) (type of data, purposes and recipients). For example, is additional information necessary when this is clear on the face of the personal data? Is it sufficient to provide a copy of the data controller's data protection notification or data protection policy?

Q3. Does the code adequately explain what will happen if an organisation does not comply with its legal obligations around subject access?

Yes.

Q4. Does the code adequately explain the circumstances when an organisation may not be required to comply with a subject access request?

Yes. However:

- this is subject to the comments above on excessively broad subject access requests; and
- it would be helpful to have further guidance on the impact of Durant v FSA when responding to subject access requests. For example, some practical examples of what sort of emails are likely to contain personal information and which are not. It might be possible to reproduce or cross reference to the Information Commissioner's guidance on access to information held in complaint files which contains a helpful summary of the position.

Q5. Do you think the code has enough good practice advice and/or practical examples?

No. See the suggestions in the submission above for further examples. It would also be useful to have an example that deals with a subject access request for personal data in a 'whistleblowing' system – particularly the interaction between the data protection rights of the person making a report and the person about whom the report is made.

Q6. Are there any sections in the code which you think need more detail?

Yes. See above.

Q7. Is the code easy to understand?

Yes.

Q8. Is there anything else the code should cover, or are there any other ways in which the code could be improved?

No further comments.

Q9. Do you agree that it will be unnecessary to retain this guidance following publication of the code?

Yes.

E felicity.banks@icaew.com