Information Commissioner's Office

Consultation:
Subject access code of practice

Start date: 29 November 2012

ico.
Information Commissioner's Office

Introduction

Introducing our consultation on the draft Subject access code of practice

The Information Commissioner's draft code of practice on subject access explains the rights that individuals have to access their personal data under the Data Protection Act 1998. It clarifies what data controllers must do to comply with their duties in providing access to personal information.

This code is intended to help organisations to provide subject access in accordance with the law and good practice. It aims to do this by explaining how to recognise a subject access request and by offering practical advice about how to deal with, and respond to, such a request. It provides guidance on the limited circumstances in which personal data is exempt from subject access. The code also explains how the right of subject access can be enforced when things go wrong.

The code will draw together a range of issues relating to subject access into one document, replacing the Information Commissioner's existing published guidance on subject access.

View the draft code of practice

The purpose and scope of this consultation

We are consulting on the draft version of the subject access code of practice to gather the views of individuals, stakeholders and organisations who process personal data. These views will inform the final published version of the code of practice.

The consultation will play an important role in ensuring the new code achieves the right balance between the protection of individuals' privacy and proportionate obligations for organisations.

The final document

The closing date of this consultation is 21 February 2013 We are aiming to publish the final code of practice by April 2013.

The document will be published on the ICO website and hard copies can be made available upon request.

A summary of consultation responses will also be published on the ICO website at the same time.

How to take part in this consultation

We welcome your responses to this consultation paper.

Responses to this consultation must be submitted by 21 February 2013. You can submit your responses in one of the following ways:

> **Download this document and email to consultations@ico.gsi.gov.uk**.
>
> **Print off this document and post to:** Data Protection Policy Delivery Team, Information Commissioner's Office, Wycliffe House, Water Lane, Cheshire, SK9 5AF; **or fax a copy to** 01625 545808.
>
> **Request a copy of this document to be posted to you and post or fax it back to us.** To request a copy, you can either telephone 0303 123 1113 and ask to speak to a member of the Data Protection Policy Delivery team, or email consultations@ico.gsi.gov.uk.
>
> Please post back your completed document to Data Protection Policy Delivery Team, Information Commissioner's Office, Wycliffe House, Water Lane, Cheshire, SK9 5AF. Alternatively, or you can fax a copy to 01625 545808.

If you would like further information on the subject access code of practice, or would like a copy of the draft code of practice and/or consultation document in an alternative format, please telephone

0303 123 1113 and ask to speak to a member of the Data Protection Policy Delivery team, or email consultations@ico.gsi.gov.uk.

Accessibility

The ICO has a Translations Policy that covers its publications. The policy states that, on request, the ICO will arrange for written information to be made available in Braille or in audit format for blind or visually impaired users.

The ICO website also has a Browsealoud feature that reads web pages for people who find it difficult to read online.

We do not translate all publications as a matter of course, but we will respond to individual requests in line with our Translations Policy, which can be found on our website.

Privacy statement

Following the end of the consultation we shall publish a paper summarising the responses. Information you provide in your response to this consultation, including personal information, may be published or disclosed in accordance with the Freedom of Information Act 2000 and the Data Protection Act 1998. If you want the information that you provide to be treated as confidential, please tell us but be aware that, under the FOIA, we cannot guarantee confidentiality.

Section 1: Your views

Please provide us with your views by answering the following questions.

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

☐ Yes

☒ No

Please explain why: The proposed Code is currently drafted with an emphasis on providing guidance to data controllers. In the ELA's view, the Code is the opportunity for the ICO to provide guidance, not only to data controllers responding to SARs but also to data subjects making SARs.

No guidance is given as to the purpose of subject access rights. In the experience of ELA members, it has become increasingly common for the right of data subjects to request access to their personal data to be used for the purposes of seeking evidence to support a tactical or legal position, rather than to verify the accuracy of personal data. Employers query the extent to which this reflects Recital 41 of the Directive, which makes clear that individuals must be able to exercise the right of access to data relating to themselves which are being processed "in order to verify in particular the accuracy of the data and the lawfulness of the processing". Employees appear to interpret this very widely. The ICO may agree with such an interpretation but it would assist ELA members were this to be explicity stated and explained.

This is particularly so because whilst the Act itself does not provide an explicit limit on the purposes for which a subject access request may be made,

the Courts have attempted to provide guidance to employers. In the ELA's view, there is confusion between the guidance provided by the Courts in cases such as Durant v. Financial Services Authority [2003] EWCA CiC1746 and Elliott v. Lloyds TSB Bank PLC and another [2012] EW Misc 7 (CC) and the technical guidance provided by the ICO. In particular, the Courts have stated that the right under section 7 of the Data Protection Act is "is to enable [a data subject] to check whether the data controller's processing of it unlawfully infringes his privacy and, if so, to take such steps as the Act provides" (Durant per Auld J para 27). Employers whom ELA members advise generally believe the position of the Courts appears to reflect the purpose of the legislation set out in the recitals to the Directive. Employees advised by ELA generally favour the wider approach. These opposing views increase uncertainty and thus cost and expense for all parties.

ELA requests that that ICO takes this opportunity to state clearly its interpretation of the purpose of data subject access requests (SARs). The draft Code of Practice ("the Code") (at page 49) states that the ICO does not accept the proposition in Durant that data controllers may refuse to comply with a subject access request where the applicant is contemplating or has already begun legal proceedings. This may remain the ICO's view and if so it should be restated and guidance given to employers and employees in the light of that view as to the purpose of the legislation to enable both responses and requests to be properly formulated. The ICO will be aware of the extent to which the right is exercised to obtain evidence in disputes and it should state its view on the legitimacy of this.

2. 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

☒ No

Please explain why: As recognised by the draft Code, a key challenge for employers when responding to DSARs is the conduct of the search of electronic files in order to locate the requester's personal data. Regrettably, the principle of "proportionality" which is a cornerstone of the processing of an individual's personal data does not feature as part of the obligations when taking steps to respond to a DSAR except in the production of the eventual response and not at the generally more onerous stage of the search for date.

Challenges in Conducting the Search

From a practical perspective, the search for personal data is very often a burdensome exercise in terms of time and cost when taking account of the large volumes of e-mails which a typical employee will send or receive (or be copied on) during the course of an employment relationship. These e-mails may or may not contain the requester's personal data for the purposes of the DPA 1998; indeed in light of the decision in Durant and the ICO's Technical Guidance on the definition of personal data, it may be that the majority of such e-mails generated through the individual's performance of their duties of employment will not contain their personal data or the data of any third party. Nonetheless, all such e-mails processed by the employer will potentially need to be reviewed in order to respond to a DSAR.

In the experience of ELA members advising employers, even the most sophisticated employers do not have IT systems which enable them to conduct an automated search of e-mails in a manner which accurately distinguishes between those which contain the requester's personal data and those which do not. The use of key words to search electronic documents can sometimes assist with the task of locating relevant files containing the requester's personal data. However, the volume of e-mails in question often results in a large

volume of "false positive" results when using key words, so the task remains burdensome.

The challenge is exacerbated for employers who operated in regulated environments, such as the financial services sector, where they are subject to stringent requirements to retain comprehensive copies of all electronic files (including e-mails) as part of their archive and back up systems. In these cases, it will often be necessary to go through a costly and time consuming process to restore the data before it can searched for e-mails which potentially contain the requester's personal data.

Costs Issues

Following on from the above, the costs for employers in responding to a DSAR can be very significant indeed. Anecdotally, ELA members acting for employers reported that these costs can range from a couple of thousand pounds in straightforward cases to six figure sums in the most extreme cases (which inevitably involve broadly framed requests and the retrieval of significant quantities of data from archive systems).

These costs are incurred in a number of different ways:

- direct management and personnel costs for retrieving, searching and reviewing potentially relevant files in order to locate the requester's personal data;

- external costs for taking legal advice on responding to the DSAR and, in particular, on technical issues such as the definition of personal data, the application of the exemption for legally privileged material and dealing with the personal data of third parties; and

- external costs for instructing specialist IT consultants to assist with the retrieval of archived or deleted data and/or to assist with the search for relevant items (for example, by removing duplicate items).

Practical Consequences

The practical consequence of the challenges set out above is that there are huge variances in the approach taken by different employers to complying with their

obligations when responding to a DSAR. Employees therefore can expect completely different and apparently random levels of response between different employers. Save for in the most straightforward of cases, employers are faced with the unsatisfactory choice of either undertaking a disproportionately costly and burdensome search and review exercise in order to deal with the DSAR, or alternatively to respond in a manner which may not fulfil its obligations under Section 7 of the DPA as interpreted by existing ICO guidance. ELA is aware of many examples where employers have felt frustrated when dealing with a DSAR as, from an organisational and cultural perspective, they are concerned to be compliant with their full range of obligations under the DPA, yet comprehensive compliance with their DSAR obligations is not realistic in practice.

Suggestions for Modifications to the Draft Code

ELA considers that there are two key areas in which the draft Code could be revised in order to address the challenges detailed above and to provide employers with a clearer and more practical framework for compliance and thus employees with more certainty and consistency in responses.

Suggestion 1: Clarifying the Request (page 24)

The draft Code includes commentary in Section 6 (page 24 onwards) on the use of Section 7(3) of the DPA to ask the requester for information that is reasonably needed to locate the personal data covered by the request. Indeed, employers faced with broad DSARs often rely on this provision to request additional information from the requester with a view to narrowing the request in terms of date ranges, topics, key words or particular IT users.

Unfortunately, the appropriate parameters of a clarification request under section 7(3) DPA remain unclear, and the guidance set out in the draft Code at pages 24 to 26 provides considerable scope for confusion over what steps an employer can legitimately take in order to respond a DSAR which has been submitted in the broadest of terms. The Code makes it clear that a requester cannot be asked to narrow the scope of their request and that they are entitled to ask for "all the information you hold" about them. However it is unclear

as to how far an employer can go to require the requester to identify particular date ranges, subject matters or (in the case of e-mails) senders/recipients in order to locate the particular personal data which they are seeking.

In the scenario where an employer holds tens of thousands of e-mails which potentially contain the personal data of the requester, as a matter of practicality it will be necessary for the requester to narrow the scope of the request in order for the employer to meaningfully comply; providing the requester "all the information you hold" is not a realistic option in these cases. However, it is ELA's experience that requesters are often reluctant to provide detailed information which can be used to narrow the scope of the employer's search based on suspicion of the employer's motive in taking this step. Consequently, clarification requests from an employer can sometimes result in an impasse between the parties and a complaint to the ICO requesting action, which is unsatisfactory for requester, responder and the ICO.

Following on from the above, ELA considers that the draft Code should:

- include additional guidance for employers on the use of Section 7(3) of the DPA as a tool to ensure that they are able to conduct targeted and effective searches for a requester's personal data in response to a DSAR;

- place greater emphasis on requesters cooperating where possible with clarification requests from employers under 7(3) DPA by providing information which assists the employer to target the particular category or categories of personal data which they are seeking.

Suggestion 2: Archived Information and Back-Up Records (page 26)

The draft Code recognises the distinction between information stored on "live" files, versus information on stored archive, back-up or deleted items systems. On this point, the Code draws a further distinction for files which have been deleted but capable of retrieval through technological measures, and suggests that the ICO would not expect organisations to use extreme measures to reconstitute such data in order to respond

to a DSAR.

On this issue, ELA considers that a similar principle should apply to data which has been removed from an employer's "live" system and archived or stored on a back up file in a form which is not readily or accessible to the employer. For most large organisations, it is the retrieval and review of these archive and back up files which is the most costly and time-consuming aspect of responding to a DSAR. This retrieval exercise, followed by the necessary filtering and de-duplication of the results, will sometimes involve the same level of difficulty as reconstituting deleted data. The Code could emphasise that employers should not adopt artificial archiving policies as a means of constraining DSAR's.

In this regard, the ICO's observations relating to data held in deleted files apply equally to personal data stored on the archive/back up files in that it is not being used to make decisions affecting the requester and any inaccuracies can have no effect as the information is not readily accessible to the employer or any other persons. As such, the fact that the requester's personal data is being processed on these archive/back up files has little (if any) impact on their privacy. Accordingly, the Working Party considers that the ICO's sensible conclusions relating to the reconstitution of deleted files when responding to a DSAR should apply equally to the reconstitution of data on archived and back up files which is not capable of easy retrieval.

Finally, the Code is insufficiently clear as to a respondent's obligations when there are pending or actual legal proceedings between the requestor and the recipient, given the apparent inconsistency between the ICO's views and those of the Courts. This should be expressly addressed.

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

☐ Yes

☒ No

Please explain why: ELA infers from the relatively

small number of cases in which it appears the ICO has taken enforcement action that it will use its powers sparingly. If that is correct it would assist both requesters and responders to understand the circumstances in which the ICO is likely to take action, accepting that the ICO retains discretion to act as it thinks appropriate.

ELA believes that Section 11 of the Code (Enforcing the right of subject access) should not give data subjects an unrealistic expectation of either the appetite of the ICO to exercise its enforcement powers in relation to relatively minor breaches of the DPA or of the resources that the ICO has available to it. ELA notes that for employers in the public sector or those who contract with that sector, the impact of any sanction can be very major indeed: in the latter case it can prevent companies proceeding with tenders for work on the basis of regulatory non-compliance. However, private sector employers apparently have much less to fear. This leads to obvious unfairness for requesters, the response to whom may be shaped as much by the sector in which they work as it is by the requirements of law or the Code.

ELA notes the confirmation that the ICO will not take enforcement action where a data controller fails to search archived systems if no evidence that it differs from the live system (p27). However in view of the RAP objectives of transparency and proportionality ELA believes that it would be helpful to have further examples of when the ICO would be unlikely to exercise its enforcement powers.

For example it might be the policy of the ICO that action would not be taken in the following circumstances:

- a data controller has a clear procedure for how SARs should be made but the SAR is made to another person within the organisation (unless the

SAR was clearly expressed to be such).

- a data controller misses the 40 day time limit for a good reason provided they manage the data subject's expectations and there is no prejudice to the data subject (NB in Ezsias the High Court held that there was no damage or prejudice as a result of the time limit being breached and it might be helpful to refer to this finding in the Code).

- a data controller carries out a reasonable and proportionate search.

The Code acknowledges that the Courts are reluctant to exercise their discretion to enforce the right to make a subject access request where it is made for an improper purpose such as to further litigation (page 50).
However the Code suggests that the DPA still requires a data controller to comply. It would be especially helpful to have a clear statement of whether or not the ICO will seek to exercise its enforcement powers in these circumstances.

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

☐ Yes

☒ No

Please explain why: See 1 above. In addition, and importantly, Section 9 of the draft code is unclear in this respect as to whether or not an organisation has to comply with the subject access request where the information requested is in connection with actual or potential legal proceedings. The paragraphs dealing with actual or legal proceedings are in Section 9 under exemptions but the text plainly records that there is no exemption in such circumstances. This is misleading.

On the one hand the code states that "you may not

refuse to supply information" and that the DPA contains no exemption for such information. However, the guidance goes on to say that the ICO recognises that the courts have discretion as to whether or not to order compliance with a subject access request. Basically, the message appears to be that the ICO says that compliance must occur but then also says this compliance may not be enforced. This cannot be an acceptable approach to a code of conduct. There is no guidance as to when a court might enforce and when they might not and no guidance on factors which might be taken into account in exercising that discretion. In addition, there is no guidance as to what the ICO. might take into account when looking at issuing an enforcement notice.

We would suggest that guidance is given as to what might be taken into consideration by the court:

- timing – what stage the litigation is at – whether it is potential or actual is likely to be highly relevant. If disclosure is imminent or has already taken place the court will address the reasonableness of the obligation to comply with the subject access request in those circumstances

- the degree of similarity between the documentation requested under the subject access request and documentation relevant to the litigation and therefore disclosable

- the purpose of the request – if it is to address some concern about the way that data has been handled or stored it would be likely that a court would enforce as opposed to where there appears to be no purpose other than to obtain documentation relevant to the litigation.

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

☐ Yes

☒ No

Please explain why: Whilst a breach of the recommendations themselves will not necessarily constitute a breach of the draft Code, the ICO is clear that the draft Code is the ICO's "interpretation of what the DPA requires of organisations to comply with SARs" (Chapter 1. About this Code, page 5).

In the light of the importance of the recommendations in addressing compliance, we have considered the scope of these in some detail. ELA has also considered whether there are any additional areas where good practice recommendations would be useful in order to assist organisations in understanding and complying with their obligations.

A number of the recommendations are very wide ranging, going far beyond what would be practical or feasible in any but the very largest, consumer-facing organisations (see below). In ELA's view the inclusion of these very broad recommendations undermines the remainder of the generally helpful suggestions and may also operate as a broader disincentive to comply for a good proportion of data controllers. .

- Chapter 3: Taking a Positive Attitude - "Request handling staff" / "Data protection experts" / "Monitoring compliance" - taken together, these three recommendations suggest a three tier structure in organisations to address a SAR / data protection issues. For the vast majority of data controllers this is impractical and costly - leading to a situation where most data controllers will not be able to comply with the recommendation. The suggestion that organisations have "Information Governance

Steering Group" meetings are similarly impractical.

- Chapter 5: Responding to a subject access request - Whilst ELA acknowledges that having standard file naming conventions for electronic documents would assist greatly in the search for personal data in the context of a SAR (page 18), this is likely to be difficult for data controllers to implement and police. Furthermore, the significant efforts the guidance suggests are required to locate relevant data would appear to suggest that a data controller could not in any case rely on such naming conventions to locate relevant data. In any case, if a data controller has not had standard naming conventions in place previously, it will be practically impossible to implement this process retrospectively, reducing the effectiveness of such a system.

- Chapter 5: Responding to a subject access request - "Systems, technology and contracts" (page 22) - A similar point to that made above arises in relation to the recommendation to have reliable file contents pages, descriptions of documents and metadata. ELA is unaware of the existence of a dedicated IT system which can manage (in the sense of carrying out relevant searches) and monitor the status of SARs and, in any case, would only expect to see such a system in the very largest (typically consumer-facing) organisations. It would be more helpful for the draft Code to include guidance on the type of system the vast majority of data controllers would expect to have in place, rather than one expected of a very small minority. We assume this could be a simple database or spreadsheet, tracking key dates / milestones.

- Chapter 6: Finding and retrieving the relevant information - "Asset registers" (page 30) - In ELA's experience, the vast majority of data controllers would not consider it practical to draw

up and maintain an asset register as suggested - it would be either too generic (listing types of data / storage locations in very general terms e.g. personnel records, HR) and therefore of little or no value, or would otherwise necessarily be too detailed, requiring a great deal of time, cost and effort to create and maintain. This may therefore be another situation where the overwhelming majority of data controllers fail to comply with one of the good practice recommendations, diluting the effectiveness of the remainder.

- Chapter 4: Recognising a subject access request - The draft Code states that SARs might validly be received, amongst other means, via an organisation's Facebook page or Twitter account (page 10). In practice, a good number of Twitter and Facebook users use pseudonyms, and there is also a potential problem of users pretending to be someone other than their true identity. Data controllers will therefore almost inevitably have to seek proof of identity from the requester, most likely through more traditional means. ELA therefore questions the merit of including a statement to this effect in the draft Code.

- Chapter 9: Exemptions - We consider that users of the Code (both requesters and responders) are likely to benefit from the explanation of subject access requests in the context of legal proceedings, since it is our experience that that is the context in which such requests are most commonly made. Although it is outside the scope of this consultation, it would appear to us that the volume of such requests could be substantially reduced if the response time were amended from 40 days to 3 months, since that latter period represents the time limit for most claims in the Employment Tribunal. In this way, data subjects would be encouraged to use the subject access regime only for the purpose for which it was enacted, and not as a means to obtain

pre-action disclosure.

Once again, however, ELA notes that the good practice recommendations set out in this chapter appear to suggest a level of dedicated staff resource beyond the realms of most data controllers. The Commissioner appears to suggest that information redacted by one person is then approved by a further person before finally being reviewed and approved by "at least one" manager to confirm its removal. This three-tier approach appears to anticipate that, in order to comply with best practice, any data controller will require not only dedicated management support to deal with subject access requests, but also a significant hierarchy of administrators.

Going further than legally required

- Chapter 5: Responding to a subject access request - "Managing Expectations" (page 22) - The draft Code indicates that it would be good practice to provide an explanation of the searches which have been made to deal with a SAR, together with the information revealed by the searches. This recommendation goes further than required by the DPA and, in ELA's experience, provision of this level of detail frequently leads to a time consuming dispute about the scope and extent of the searches undertaken.

- Chapter 8: Supplying Information to the requester - "Online and electronic formats" and "Copy differentiation" (page 42) - The recommendations at the end of Chapter 8 again appear to suggest steps far beyond the requirements of the DPA, which may be unduly burdensome. The draft Code suggests, for example, that information should be supplied in machine-readable form if so requested. Where personal data is held in handwritten notes, for example (as is common), we would question whether it is realistic to expect respondents to

assign valuable time within the limited 40-day response period to effectively typing up copies of those notes. Similarly, we would question whether stamping a document "data subject copy" is likely to make any material difference to the ability to identify the source of any data leak.

Clarification required

- Chapter 7: Dealing with subject access requests involving other people's information - the guidance provided in this chapter appears to conflate the concept of third party personal data, and "information which relates to and identifies a third party individual". It is ELA's understanding that those two concepts are distinct, and the guidance is therefore potentially confusing.

s.7(4) DPA, which defines the concept of third party information in respect of which this guidance is provided, refers to information relating to another individual who can be identified from that information. This appears to be at once both narrower and wider than the concept of personal data. It is limited to information from which the relevant individual can be identified (i.e. without reference to any other information in the data controller's possession), but also arguably extends beyond data which is about someone in a biographical sense to data which merely relates to them. In our view, users of the Code of Practice are likely to benefit from clarification of this distinction, emphasising that the guidance on disclosure of third party data extends beyond third party personal data to all data relating to a third party who can be identified from it.

- Chapter 8: Supplying Information to the requester - Reference is made in this section to the obligation pursuant to s.7(1)(b) DPA to provide, where requested, a description of the personal data, the reasons why it is being processed, and the recipients or classes of recipients to whom the

data may be disclosed. It is our experience that such questions are routinely asked not out of a genuine desire to understand the answers to those questions, but as a means of imposing a greater administrative burden on the respondent, particularly where the request is made in the context of potential litigation.

In ELA's experience, respondents are often confused as to the degree of detail which is required to be provided in response to such questions. In some cases, respondents (in our view incorrectly) consider it effectively requires a separate response to such questions in respect of each and every individual document, which would of course represent an extremely burdensome requirement. In light of the typically somewhat tactical nature of such requests, and the confusion that permeates this area, it is our view that users of the Code would benefit from a practical example of the type of response that the Commissioner would expect to see. However, in light of our comments above regarding the practicability of certain of the recommendations set out in this draft Code, we would highlight the need for such guidance to be practical and realistic, so as to ensure that the Code is not held out as an unrealistic measure of perfection that can never be achieved in practice.

In addition, where litigation is pending or contemplated, organisations should be encouraged to use a checklist approach where litigation is pending or actual so that the factors set out in 4. can be applied in every case and recorded when deciding whether or not it is necessary to comply.

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

☒ Yes

Please give details: See our response generally but in particular ELA would welcome more detail in the

paragraphs dealing with how to respond when there are actual or contemplated legal proceedings.

☐ No

7. Is the code easy to understand?

☒ Yes

☐ No

Please explain why: We assume this question is directed at the clarity of the language used in the code, which is good. However, please see our other comments on the substantive clarity of the document.

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

☒ Yes

Please give details: It should be clearer that the Code is addressed to data controllers and not data processors. The distinction is not well understood and the Code repeatedly refers to "you must". In section 1, the Code states "any organisation which holds personal data should use this Code…" and in Section 5 it suggests that a data processor is required to deal with an SAR (which they are not unless there is a contractual requirement to do so).

- Section 2: "What information is an individual entitled to" It might be helpful to remind businesses that they may breach commercial confidentiality obligations and possibly lose the benefit of legal privilege if they disclose other information as part of responding to an SAR.

- Section 4: "Requests made on behalf of others". It may be helpful to clarify that it is usually appropriate to assume that a solicitor listed

on the SRA website acts for the person they say they act for.

- Section 8: "Supplying information to the requester". SARs are usually returned by post. Is there any obligation to use recorded delivery or other secure methods of delivery?

- Section 7: "Confidentiality". This section of the Code confusingly implies that a duty of confidentiality between an employer and employee may justify non-disclosure. Section 7(4) only applies where the disclosure would involve the disclosure of personal data relating to another data subject and so this could only be relevant where another employee was an individual data subject. The Code should also make it clear that information covered by legal confidentiality is likely to be privileged and so is subject to an absolute exception

In addition, the Code should clarify the extent to which any search should extend to group companies - the draft Code does address the situation in relation to a third party (page 18), and ELA is of the view that this example could easily be extended to address this issue;

There should also be confirmation that there is no obligation for an independent person within the organisation to conduct a search for the relevant data in a SAR scenario (i.e. it is possible to approach individual line managers, or those with direct dealings with the data subject, for example, to request that they carry out the relevant searches).

If there is no exemption from providing a response to a subject access request where there is actual or pending litigation then it is misleading to place the legal proceedings section under section 9 – "Exemptions". The legal advice section dealing with privileged documents should be separate from the advice on whether or not to comply where there are potential or actual legal proceedings

☐ No

9. The code will replace the following existing pieces of guidance relating to subject access on our website:

- **Disproportionate effort – section 8(2)**
- **Subject access to health records by members of the public**
- **Checklist for handling requests for personal information**
- **Subject access and employment references**
- **Subject access requests and legal proceedings**
- **Dealing with subject access requests involving other people's information**

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

☒ Yes

☐ No

Please explain why: For the guidance to be effective, it must be easily accessible. Respondents must be able to find it from a single source. It follows that any amendments to the Code or any statements relating to it must be appended to the document or clearly linked as being related on the ICO's website.

Section 2: About you

1. Are you:

	√
A member of the public who has used our service?	
A member of the public who has not used our service?	
A representative of a public sector organisation? Please specify:	
A representative of a private sector organisation? Please specify:	
A representative of a community, voluntary or charitable organisation, or of a trade body? Please specify: The Employment Lawyers Association ("ELA") is a non-political group of approximately 6,000 specialists in the field of employment law and includes those who represent claimants and respondents in courts and employment tribunals. It is therefore not ELA's role to comment on the political merits or otherwise of proposed legislation, rather to make observations from a legal standpoint. ELA's Legislative and 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. The Legislative and Policy Committee of the ELA set up a sub-committee under the chairmanship of Jonathan Chamberlain of Wragge & Co to consider and comment on the consultation paper Subject Access Code of	

Practice published by ICO in November 2012. A full list of the members of the subcommittee is set out below. Members of the ELA sub-committee Jonathan Chamberlain, Wragge & Co (Chair) James English, Samuel Phillips Solicitors Suzanne Horne, Paul Hastings LLP Marc Jones, Turbervilles Solicitors Rebecca Kershaw, Barlow Robbins LLP Timothy Pitt-Payne, 11 KBW Daniel Pollard, Macfarlanes LLP Anya Proops, 11 KBW Stephen Ratcliffe, Baker & McKenzie LLP Khurram Shamsee, DAC Beachcroft LLP Anna Shelley, Simmons & Simmons LLP Caroline Stroud, Freshfield Bruckhaus Deringer LLP	
Other? Please specify:	

Thank you for completing this consultation.
We value your input.