EMPLOYMENT
LAWYERS
ASSOCIATION

PO Box 1609
High Wycombe
HP11 9NG
TELEPHONE 01895 256972
E-MAIL ela@elaweb.org.uk
WEBSITE
www.elaweb.org.uk

ICO Consultation on the draft right of access guidance

Response from the Employment Lawyers Association

12 February 2020

EMPLOYMENT
LAWYERS
ASSOCIATION

ICO Consultation on the draft right of access guidance

Response from the Employment Lawyers Association

12 February 2020

Introduction

The Employment Lawyers Association ("ELA") is a non-political group of specialists in the field of employment law and includes those who represent claimants and respondents in courts and employment tribunals. It is not ELA's role to comment on the political or policy merits or otherwise of proposed legislation or regulation, rather it is to make observations from a legal standpoint. Accordingly, in this consultation we do not address such issues. Further, given the membership of our organisation, it has not been possible to answer all questions in this consultation which were targeted directly at employer/employee representative bodies

ELA's Legislative and Policy Committee consists of experienced solicitors and barristers who meet regularly for a number of purposes including to consider and respond to proposed legislation and regulations.

A working party, co-chaired by [redacted] and [redacted] was set up by the Legislative and Policy Committee of ELA to respond to the draft ICO Guidance on DSARs. Members of the ELA working party are listed at the end of this paper.

Q1

Does the draft guidance cover the relevant issues about the right of access?

Yes

No

Unsure/don't know

If no, unsure/don't know what other issues would you like to be covered in it?

No. The draft guidance does cover some relevant issues about the right of access, however, we consider that additional information is required in relation to the following points:

- We consider it might be appropriate to insert the following wording in the "About this detailed guidance" section on page two (similar to that found in the guidance on the Acas Codes of Practice as a reminder of their non-binding status):

"Please note that legal information is provided for guidance only and should not be regarded as an authoritative statement of the law, which can only be made by reference to the particular circumstances which apply. It may, therefore, be wise to seek legal advice".

- **"*Other supplementary information*" under *"What is an individual entitled to?"*** p. 3. We consider it would be useful to state that other supplementary information, for example purposes for processing, categories of data and retention periods, must be supplied as mandatory each time an organisation responds to a SAR, even if it is not requested by the individual.

- Under the "***Who is responsible for responding to a request?***" p. 5, it would be useful to cover the fact that contractual arrangements between a controller and processor should cover the processor's duty to assist with a SAR, but controllers are not permitted to extend the time period to respond to a SAR, merely because a processor is involved, nor pass on the duty to respond to the processor. It is also worth noting that in light of the Attorney General's opinion on the validity of standard contractual clauses, scrutiny may be heightened around how controllers monitor their processor's ability to *practically* comply with the with the terms of SCCs.

- Under "***Should we provide a standard form for individuals to make a request?***", p. 10 we recommend that, in addition to referring to a template SAR form, the guidance makes reference to the option of a data controller preparing other standardised letters to provide to individuals to help streamline the request process for both parties and ensure basic information is provided in a timely manner. For example, early initial communications acknowledging receipt of the SAR, requests for identity verification and templates supplying the information requested. Tailoring such documentation would be required in each case. This paper trail would also assist with accountability later.

- The draft guidance should address the complexities of bring your own devices ("BYOD") in the employment context. Members of staff routinely communicate on personal devices but these communications, which may include a data subject's personal data, can often be in a non-work capacity and context.

  The final sentence of the section states: "We do not expect you to instruct staff to search their private emails or personal devices in response to a SAR unless you have good reason to believe they are holding relevant personal data". At a minimum, we would suggest that this sentence needs to be amended as follows: "We do not expect you to instruct staff to search their private emails or personal devices in response to a SAR unless you have good reason to believe they are holding relevant personal data which they are processing on your behalf".

  It would also be useful to include additional guidance on what the ICO considers to be a 'good reason' to believe a staff member is holding relevant personal data on a personal device – this might be addressed through including an additional example with an employment context. Guidance on whether employers are obliged to search WhatsApp and other instant messages on company mobile phones in the context of a DSAR would be helpful, taking into account the risk of significant intrusion into another individual's private life and the impact of the Computer Misuse Act. Policies on recordings should be mentioned to cover CCTV and/or recorded calls and consider how they will link to the SAR process.

- Guidance on the issue of document metadata would be helpful i.e. to show when personal data might have been prepared or modified. Specifically, we consider it would be helpful to include further detail on whether there is any obligation to provide metadata in the ordinary course of responding to a SAR, (noting that this is potentially very onerous).

- Further guidance would also be helpful on the issue of data held in different languages e.g. if employees are on assignment in UK offices and have used other languages to correspond. We consider it would be helpful to have further guidance on how organisations might deal with such circumstances and whether there is an obligation on organisations to translate such data, should it be relevant to the SAR.

- Further guidance on responding to requests about children or young people. Assuming a child is under 12, they may not have "sufficient age and maturity to exercise their rights". Clarity of the process for responding to requests made by, for example, parents of children under 3 years of age, would be useful. For example, is it sufficient to consider the child's age alone that it clearly must be in the best interests of the child to respond to someone with parental responsibility? How does the parental responsibility need to be proven/satisfied, if at all?

- Under "***How long do we have to comply***" p. 16, the guidance adopts recent revisions to the ICO's Guide to the GDPR. This change in approach is potentially problematic for controllers who process large volumes of data as part of their archives, particularly in the regulated sector (e.g. financial services), where the provision of such information is often critical in order for the controller to complete a proper search for the personal data within the relevant one/three month timescale. The previous ICO position enabled both parties to meaningfully engage with one another to clarify the request. Under the proposed approach, there is also a very real possibility that an employee could clarify the request when an employer is at an advanced stage in locating the data after performing reasonable searches. Where the data subject's clarification is not in alignment with the steps the data controller has already taken, this would result in unnecessary time and cost expenditure in locating personal data the data subject eventually confirms he/she does not wish to receive a copy of. In addition, in cases where a data subject makes a very wide request to a data controller which processes a large volume of data, further information from the data subject is often needed **before** the data controller can undertake a retrieval of data from its archives. We note that a data controller can still request such information, but a delay on the part of the data subject in responding is likely to prejudice the data controller's ability to complete the response within the requisite timescale.

  We consider it would be helpful to include an explanation of the change in the ICO's position in light of the following:

  - the main provisions of the GDPR are silent on this point but in Recital 63 there is reference to the fact that, where a controller processes a large quantity of information concerning the data subject, it should be able to request **before the information is delivered** that the subject specify the information or processing activities to which the request relates; and

  - the provisions of the DPA 2018 relating to SARs in the intelligence services context (sections 94(5)(a)(ii) and 95(14) DPA 2018) stipulate that the

timescale for compliance will not commence until any further information requested by the data controller is provided, so there is a mismatch between SARs made in this and other contexts (with no apparent logical basis for a distinction).

- It may be helpful to provide guidance on whether a DSAR is excessive by reference to the difficulties in retrieving information responsive to a broad request where the data is stored across the different forms of electronic media such as different IT systems, third-party processor storage systems, voicemail, call recordings, video recordings, archived systems.

- Further guidance would be helpful on what is considered a reasonable fee to charge to comply with a SAR e.g. is the figure based on the previous £10 fee under the DPA 1998, or should other practical factors be considered such as a cost per page for photocopying, printing or scanning? A worked example would also be helpful here.

- Further guidance would be helpful to include practical steps that should be taken, if an organisation does not hold any data relating to the request/individual.

- Further clarity on when the extending the time to respond to a SAR is required here. Extending time because an organisation has "recorded a number of requests" appears to be vague and uncertain and an organisation could use this to argue an extension if for example the individual makes two SARs when this is clearly not the purpose of the legislation. It would be helpful to have clarification of whether relying on the "excessive" ground necessitates other requests for data having been made and, if yes, whether they be ongoing (instead of completed) and/or overlapping for the new DSAR to be "excessive".

- Confirmation of whether the controller needs to do anything at all to respond to the request which it refuses to comply with e.g. provide the Article 15 summary of processing, if not provide the actual data or conduct any searches prior to confirming.

- It would also be helpful to have further clarity on whether motive for a SAR is relevant to determining whether a SAR is "manifestly unfounded".

- SARs in the employment context are often in the context of a dispute. This means that, in many cases, the information an employee is seeking may have legal, professional or personal implications for third parties whose data is also contained in e.g. emails containing the data subject's data. For example, if a manager expresses a negative opinion in an email to another about the requester, the manager will likely have a strong desire to withhold the disclosure of his personal data. It would be helpful for the ICO to clarify where the balance in such cases generally lies. Does the balance shift if the manager's opinion is discriminatory or expresses an intent to retaliate against the requester for making a complaint/blowing the whistle, bearing in mind the manager could be exposed to personal legal liability?

- We consider it would be useful to include a reference to the fact that a controller may have to consider other regulatory and enforcement regimes if they operate in more than one Member State.

Q2

Does the draft guidance contain the right level of detail?

Yes

No

Unsure/don't know

If no, unsure/don't know what area should there be more detail within the draft guidance?

No. We consider further detail and clarity is required in relation to the following points:

- Whilst the reference to the Regulatory Action Policy is relevant, it may be appropriate to refer to the increased financial penalties explicitly even though they do not apply solely in relation to SARs.
- It would be useful to include guidance on the position in relation to group companies, particularly in the circumstance in which individual companies within a group operate as separate data controllers.
- The example on page 17 states that "the request is complex" indicating that the response time can be extended, but does not explain why the request is considered to be complex. Clarification on why this specific request is complex would be useful, in order to assist the reader as to what constitutes a complex request.
- **Personal data definition:** It would be helpful to include a section on what personal data is in the context of a DSAR. The long established principle in the UK courts with DSARs is it must have a "biographical significance" i.e. some sort of focus on the individual. Confirmation of the ICO's position and some examples of what would be or would not be personal data would be useful.
- Under ***What efforts should we make to find information?***, further detail is required as to the extent of the efforts data controllers should make to locate personal data. Further explanation and examples are required to define and demonstrate what is meant by the terms "high expectations" and "extensive efforts", which are terms set out in the guidance.
- In particular, the concept of "proportionality" in relation to the efforts a data controller is required to take is almost entirely absent from the guidance (save in respect of SARs via social media channels, in relation to which data controllers must "take reasonable and proportionate steps to respond effectively"). This is surprising given the express reference to proportionality in the GDPR at Recital 4(2): "*The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality*". In addition, proportionality is a general principle of EU law, enshrined in Article 5 of the Treaty of the European Union.
- We note in particular that the ICO's previous guidance under the Data Protection Act 1998 which states that data controllers "are not required to do things that would be

unreasonable or disproportionate to the importance of providing subject access to the information" has been removed. We find the omission of this statement surprising, since we do not believe that the GDPR requires (or the ICO would want) data controllers to take unreasonable or disproportionate steps. We suggest reinstating this wording and providing examples of what would and would not be considered unreasonable and disproportionate. We consider that this guidance would be helpful to guide the expectations of both data controllers (in particular those with less available resources) and data subjects.

- Further, this part of the guidance should provide more practical information on "what efforts" are necessary, for example:

  "Normally where a data subject makes a request to access their personal data, it will be necessary for data controllers to search their electronic and physical records in order to locate the relevant personal data. Depending on the circumstances, searching can be done in a number of ways, including by asking key persons to conduct a manual search for hard-copy and electronic information, or by using an electronic search tool. Searching electronic records can often be done by keywords related to the data subject's name (or other identifying information (such as a unique ID number)) and/or the topics of the SAR. Further guidance on different types of records is provided below.

  It may be appropriate for data controllers to inform the person making a SAR about the process it will follow to comply with the SAR, either at the start of the process or when responding to the SAR with the information requested".

- Guidance regarding the extent of the searches required when responding to a SAR should be determined in light of the purpose of data subject access requests. On this point, we note that a section that has been removed from the ICO's previous guidance under the Data Protection Act 1998, which stated: " ..the Information Commissioner has considered that the purpose of subject access is to enable individuals to find out what information is held about them, to check its accuracy and ensure it is up to date…". We believe this should be reinstated.

- We consider that guidance under "***Can we clarify the request?***" to be unclear. We believe the guidance in the second paragraph of this section should read: "You cannot require the requester to narrow the scope of their request" (as included in the previous guidance under the Data Protection Act 1998), rather than "cannot **ask**", as often by clarifying the request, a data controller will be indirectly asking the data subject to narrow their request. This is also envisaged as acceptable by recital 63(7) to GDPR. This is also clearly envisaged by the supermarket example on page 24 of the guidance. Further, there is nothing in the GDPR or the Data Protection Act 2018 that prohibits a data controller from requesting that the data subject narrow their request.

- Additionally, if the request is unclear and the data controller requires more information in order to provide the data to the data subject, then the time period for responding should not start running until clarification has been provided. Further detail on this is set out in Q1. At a minimum, we consider that it should be clarified that where data controllers consider that an original request is manifestly unreasonable or excessive, then the timescale for responding does not start until the request is clarified or a reasonable request is received from the data subject.

- If the ICO considers that no pause of the time to respond is appropriate as per the suggestions above, then as an absolute minimum, the guidance should provide an obligation on the data subject to respond without unreasonable delay to any requests for clarification from the data controller in order to ensure that the data controller's time for preparing its response is not unnecessarily delayed or limited. The guidance should also explain that, if the data subject does not respond to a reasonable request for clarification, the controller should be entitled to take a reasonable and proportionate approach to searches. This is particularly important in the employment context, where a request from an employee for "all my personal data" could relate to a vast quantity of data gathered during the employment relationship over a very lengthy period.

- In relation to archived information and back-up records, the ICO's previous guidance under the Data Protection Act 1998 stated that "If a request relates specifically to back-up copies of information held on your 'live' systems, it is reasonable to consider whether there is any evidence that the back-up data differs materially from that which is held on the 'live' systems and which has been supplied to the requester. If there is no evidence that there is any material difference, the Information Commissioner would not seek to enforce the right of subject access in relation to the back-up records." This was a helpful clarification and we ask that it is retained in the new guidance.

- In relation to 'deleted' information, the guidance states that "the fact that expensive technical expertise may enable it to be recreated does not mean you must go to such efforts to respond to a SAR" and "the ICO will not seek to take enforcement action against an organization that has failed to use extreme measures to recreate previously 'deleted' personal data held in electronic form". It is not clear what the ICO would consider constitutes 'expensive technical expertise' and/or 'extreme measures', or indeed whether the ICO considers that a data controller using 'expensive technical expertise' would be an 'extreme measure'. The draft guidance then goes on to state that: "We do not require organisations to use time and effort reconstituting information that they have deleted as part of their general records management".

  This latter sentence is clear and easily understandable for controllers, and we therefore consider that it would be preferable to retain this sentence and remove the references to 'expensive technical expertise' and 'extreme measures'. However, if the ICO wishes to retain these references, we suggest that it clarifies the meaning of 'expensive technical expertise' and 'extreme measures' – this clarification could take the form of a new example.

- Given that the burden on employer data controllers to search email records for personal data is immense due to the vast number of emails sent and received during the employment relationship, we consider that this section of the draft guidance should make reference to the EU law concept of proportionality and guidance around what constitutes a proportionate search. It may not, for example, be proportionate for a controller to routinely search 'non-live'/archived systems for personal data where this step is not specifically requested by a data subject.

- This guidance does not clarify whether it applies to data that may form part of a request which is held overseas or just domestically. We propose adding the following wording:

"Additionally, the right of access may extend to data stored/processed by the data controller outside the UK. Data controllers based outside the UK might also be subject to the GDPR depending on the nature of their operations (**[Suggest linking to any other appropriate ICO guidance here]**)."

- We suggest that it might be helpful to include some guidance on how the ICO would approach issues arising as a result of a multi-jurisdictional request. Notwithstanding the same basic law, the approach of courts and the equivalents of the ICO can be quite different and could lead to frustration and disappointment on the part of those making requests. It may be helpful for the guidance to point out that not every jurisdiction would follow the same approach as the UK.

- The explanation regarding the definition of a 'filing system' is very minimal. We are aware of the ICO's 2011 guidance on filing systems (i.e. the Frequently asked questions and answers about relevant filing systems, available here: https://ico.org.uk/media/for-organisations/documents/1592/relevant_filing_systems_faqs.pdf). We would suggest that a link to this or similar guidance be included in this section of the draft guidance.

- It would also be helpful for the ICO to include a new example that covers how the right to access applies to hard-copy records, including an example of how a controller determines whether such records take the form of a 'filing system'.

- The guidance under the heading "***How do we decide what information to supply?"*** states that "it may be easier (and more helpful) to give a requester a mixture of all the personal data and ordinary information relevant to their request, rather than to look at every document in a file to decide whether or not it is their personal data". However, there seems a high risk that such an approach could result in inadvertently providing the data subject with third party personal data which the third party would not reasonably expect to be made available to the requestor. As a result, our view is that this approach will rarely be reasonable or appropriate in the employment context, where in many cases documents including an employee's personal data will also contain third party personal data.

- For example, as noted in the example on page 39 of the guidance, an employee's human resources file may contain information identifying others such as managers and colleagues who have contributed to (or are discussed in) that file. We therefore suggest that this point is removed from the guidance.

- The guidance states that "although the easiest way to provide the relevant information is often to supply copies of original documents, you are not obliged to do so". We would suggest clarifying the fact that data subjects only have the right to access their personal data and not to receive copies of documents. The guidance should also make clear that, to the extent a controller provides copies of original documents, such documents can – and should where necessary – be redacted to remove information that the data subject does not have the right to receive - including exempt data and, where appropriate, third party data. We would suggest including links to the following sections of the guidance: "What should we do if the request involves information about other individuals?" and "What other exemptions are there?".

- The guidance notes that the GDPR does not define a "commonly used electronic format", stating that the term "means the format in which you supply the requester with their personal data". We would suggest that the ICO considers providing further guidance in relation to potentially appropriate format types - particularly PDF versions of documents and copies of emails, since this is the most common format used by controllers when responding to a data subject.

- In doing so, the ICO may wish to consider the European Data Protection Board's 'guidelines on the right to data portability' (available here: http://ec.europa.eu/newsroom/document.cfm?doc_id=44099), and in particular the paragraph at the top of page 18 of those guidelines which states: "where no formats are in common use for a given industry or given context, data controllers should provide personal data using commonly used open formats (e.g. XML, JSON, CSV,...) …".

- The section on providing remote access to personal data, does not expressly cover the situation where a controller has used an e-discovery platform purely for the purposes of the data subject access request, and where it provides remote access to the data through that platform to the data subject. In such circumstances, it should be made clear that the information on the e-discovery platform need only be provided for a reasonable period of time in order for the data subject to access and download that data. This prevents the data controller incurring ongoing fees to host the data on the e-discovery platform, and accords with the principles of security and data minimization.

- Further detail on data portability requests is required. A link to the following ICO guidance would be helpful to assist people understand what data portability means and how to comply with that request:

    - ICO's guidance on data portability: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-data-portability/

    - EDP - WP 242: http://ec.europa.eu/newsroom/document.cfm?doc_id=44099

    - EDP - WP242 ANNEX – Frequently Asked Questions: https://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp242_annex_en_40854.pdf

- Under **"What about confidentiality?"**, p. 41, the guidance does not cover information which may be confidential commercially, whether to the controller or another third party. Recital 63 suggests that if information is commercially sensitive (or confidential) and disclosure would prejudice the trade secrets of a controller or other third party, it may be reasonable to withhold disclosure. This would seem to be a factor that can be rolled into the three-step test at pages 40-41. Confirmation from the ICO in the guidance and any further guidance on commercially sensitive or confidential information would be welcome.

- On pages 42-43, the section on the 'education data test' is ambiguous. To meet the 'education data test' it is unclear whether individuals who are:

    - Employees of a local authority that maintains a school in England or Wales;

- Teachers at voluntary aided, foundation or foundation special schools an alternate provision Academy, independent schools or non-maintained special schools in England or Wales;
- Teachers of schools in Northern Ireland;
- Employees of an Education Authority in Northern Ireland; or
- Employees of a Catholic School in Northern Ireland

also need to satisfy the second limb of the test set out for Scottish education authorities at page 43, namely; "and the information relates to, or was supplied by the other individual in their capacity as an employee of an education authority."

It would be useful if the guidance could provide clarity on whether the ICO adopts the two limbed test for the categories of employees above (and set out at the top of page 43 of the guidance), or the single criterion of the status of the individual, would be welcome. A two-tier test would appear consistent with the 'social work data test' and 'health data test.'

- It would also be helpful to include an example of a request for all data made by an individual who works for the local authority in which they reside. Compliance with the request may require retrieval of information held by the local authority in the capacity of employer, social work authority, education authority, in relation to council tax and as administrator of housing benefit. Practical guidance on the complexity of an example of this nature, would be welcome.
- It would also be helpful for the ICO to clarify whether information that is intended to be included in a confidential reference also falls under the 'references given in confidence' exemption. It is common practice for an HR professional to seek input from managers before compiling the feedback into a reference. On many occasions such managerial input is given via email or other written communication. If such input is not included in this exemption, its purpose would be materially undermined.
- Further, is there a presumption that there is a duty on the author of the reference to mark it 'in confidence' to indicate it is within the exception? If this has not been carried out, will it remain the decision of the data controller to assess without guidance?
- Under ***"Is health data exempt if disclosure could cause serious harm?"***, further detail is required as to what constitutes 'serious harm'.
- Under ***"Is it a criminal offence to force an individual to make a SAR?",*** it should be clarified that this offence arises where an employer requires a (prospective) employee to obtain their criminal record via a SAR rather than through the established disclosure regime.
- It would be helpful to include references to each of the specific sections which deal with enforcement in the DPA 2018 and the level of penalties which are available in each case. For example, the fines that are available in the event of a breach of section 184 or section 173. Further, it would be helpful to set out an overview of the principles that would be applied by the Court and/or ICO in each case when considering whether to apply sanctions.

- In comparison to other sections of the guidance, the section on refusing to comply with a request is relatively short and does not contain worked examples as set out in other sections of the guidance or the previous ICO guidance under the DPA 1998. It would be helpful to provide examples on the circumstances under which an organisation can refuse a request fully or if it needs to comply partially.

Q3

Does the draft guidance contain enough examples?

Yes

No

Unsure/don't know

If no, unsure/don't know please provide examples you think should be included in the draft guidance.

No.

- It would be useful to have an example in the ***What is the Right of Access?*** section, of an example SAR for scene setting and so organisations can recognise key words to look out for (noting of course that there is no specific wording required). It would also be useful to have an example of a SAR sent via social media or another social media platform to demonstrate how brief a request may be.
- In relation to preparing to respond to a SAR, it would be useful to include further information on/point out the numerous resources available from the ICO including the assessment tools.
- It would be useful if the guidance could clarify its position in relation to organisation's providing a 'tiered' response to excessive SARs. For example, when in receipt of a seemingly excessive request, an organisation may respond by creating a 'tiered' assessment to documents and to satisfy the DSAR in the time available, provide 'tier 1' documents or 'gateway' docs, i.e. meeting minutes, agendas, reports, etc. (excluding emails) and then invite the requester to make a 2nd request based after having received the 1st tier documents.
- It would be useful to include an example of a "complex" request for a small or medium sized organisation, and further examples more generally of when a request can be considered "complex". Factors relevant to the employment context should be included here. Other than one's personnel file, training records, etc. the vast majority of personal data requested by employees is contained in communications (emails, instant messages, telephone recordings). Where the requester is not the sender or recipient of the relevant communications:

  (a) locating the relevant communications;

  (b) identifying the relevant personal data within those communications;

(c) determining whether the personal data should be disclosed despite it also relating to the sender/recipient;

(d) determining the application of any relevant exemptions (e.g. legal professional privilege); and

(e) applying redactions to the parts of the communications subject to an applicable exemption,

is particularly complex. This is especially so where the requester makes a broad DSAR spanning multiple custodians over a long time period (which is common in the employment context). It would be helpful if there was a specific example in the guidance of a DSAR involving a large volume of communications in which the requester is neither the sender nor the recipient and therefore an acknowledgement that this would constitute a "complex" request.

- We suggest including examples in the "How do we find and retrieve the relevant information?" and "What efforts should we make to find information?" sections of the guidance, setting out the efforts that the ICO does *not* consider the GDPR requires data controllers to take, for example:

Example 1

"A long-standing employee of an estate agents is in dispute with his boss about what commission he is due. He makes a subject access request for all information the company holds about him, including what commission he was paid on every property he has sold since he began working for the estate agency in 2001.

The estate agency only began collating information about commissions by staff member in 2009. Finding information before this date would require matching accounts records with payroll data and consulting archived electronic records. The company estimates complying with this request would take months of work.

The estate agency assesses that providing the commission information going back to 2009 would constitute a sufficiently high level of effort to honour the employee's request."

Example 2

"The employee has sent and received hundreds of thousands of emails during his 19 years of employment with the estate agents. When the company searches their email systems and electronic documents for the employee's name and other abbreviations that would identify him, the number of documents initially identified as identifying the employee amount to 300,000 items. For one person to review these emails for the employee's personal data, at the rate of 1,000 emails a day, it would take 1,154 days (just less than four and a half years in working days).

In this case, the request itself is excessive and it would be disproportionate and unreasonable for the estate agents to review to 300,000 emails. The estate agent is a small business and is not expected to hire/outsource the review of the 300,000 documents in order to respond to the request within one month (which would require 15 people working full time). Although the estate agency would be permitted to extend the deadline for compliance by a further two months given the complexity of

the request, the request remains excessive and the effort required is disproportionate.

Instead, the employer can ask the employee to clarify the scope of his request. If the employee's clarification does not significantly narrow the request, the employer can take a reasonable and proportionate approach in order to comply with the request by assuming that certain emails will be unlikely to contain personal data (such as emails sent by the employee to clients) and that other emails will be very likely to contain personal data (such as emails sent by the employee to human resources) and are entitled to focus their searches accordingly and proportionately."

Example 3

"A long standing employee who works in IT support has made a data subject access request. As part of his employment, the employee has hundreds of calls per day, to staff in all different parts of the business, all of which are recorded.

The employee submits a data subject access request asking for copies of all of their personal data (including within telephone calls) that their employer holds. The employer reasonably believes it unlikely that any such personal data will be present in the recordings of conversations where the employee is providing IT assistance to the business.

Additionally, such calls would take years to listen to, and would be disproportionate and unreasonable, expensive and time consuming to convert to text to review. Therefore, the employer is entitled to act proportionately in deciding to search emails and other filing systems, and not the audio recordings of calls. The employer should explain this to the employee and offer that if a more specific request can be made in relation to the calls, the employer will consider complying with that request."

- An example in relation to clarifying a request, would also be helpful.

Example 4

"A bank received a SAR from a long-standing employee for all the data the bank holds regarding their employment dating back 10 years. The employee has recently raised a grievance at work and is considering starting employment litigation against the bank.

The number of documents/emails which initially match a search for the employee's name would take years to review by one person or would require significant expenditure on the part of the bank to engage additional people or outsource the work in order to review the documents/emails. In such circumstances the request is excessive.

The bank explains to the employee that as the request is currently formulated the request is disproportionate and excessive, and on that basis asks the employee if it would be acceptable to the employee for it to only send them information between two particular dates and limited to certain searches. In order to avoid unnecessary delays, whilst the bank is awaiting a response it starts reasonable searches and preparation for the searches it has proposed to carry out.

The employee clarifies, without unreasonable delay, that it wants all of the information held by the bank in relation to their employment, and that their request is

not limited to a particular date range. As the original request was excessive, the employer is still only required to provide a proportionate and reasonable response in line with its restricted proposal."

- A useful example in relation to information stored in different locations might be:

  "An employer stores some data on employees in structured hard copy files, some on a centralised HR management system, and some saved locally on HR professional's computers in named folders. A data subject access request would apply to the data in all of these locations."

- P40-41 sets out a three-step approach to dealing with requests that include personal data of others. Step 2 says that, in some circumstances, it may not be appropriate to ask individuals for consent p. 40. It would be helpful to have additional examples that set out when asking for consent may be inappropriate: for example, where the data controller had already given assurances to a third party that the information would be kept confidential in the context of an employee disciplinary process.

- Step 3 of the approach asks the data controller to assess whether it is reasonable to disclose without a third party's consent (page 41). In particular, examples of where it would be reasonable to disclose where consent has been refused would be helpful. In an employment context, employers owe a duty of trust and confidence to their employees (in addition to their data protection obligations), so worked examples would help employers better understand how to apply the balance of harm test in circumstances where consent has been refused by an employee.

- It would be helpful if the guidance in this section could be updated to reflect applicable case law on requests involving information about other individuals (that has arisen since publication of the former Subject Access Code). In particular, the guidance in ***DB v GMC* [2018] EWCA Civ 1497** deals with third party data in detail: this case sets out that a "*wide margin of assessment*" is given to data controllers when balancing the competing interests of data subjects, particularly where there is "*special sensitivity*" to the data involved.

- Step 1 of the three step approach, p.40 acknowledges that where the third-party data does not form part of the requested information ('non-mixed third party data'), it ***may*** be removed. However for many workplace SARs there will be significant non-mixed third party data (for example in email chains) and removal of all of it from copy documents would be a substantial undertaking for the controller. More guidance on how to deal with non-mixed third party data might be useful here – for example, an acknowledgement that it might be proportionate to choose to leave in non-mixed third party data in some cases – such as when the data subject has seen the data anyway. On the other hand, where there are clear privacy concerns in respect of said data, the guidance could be clearer that the data ***should*** be removed (as opposed to ***may***).

- It would be useful to include an example of a SAR in which there is an overlap of the two statutory regimes to ensure that schools (who are often the recipient) of the DSAR, are better able to understand the difference between the two regimes.

Q4 We have found that data protection professionals often struggle with applying and defining "manifestly unfounded or excessive" subject access requests. We would like to include a wide range of examples and variety of sectors to help you. Please provide some examples of "manifestly unfounded or excessive requests" below (if applicable)

Excessive Requests

The ICO's current guidance provides that a large number of documents cannot be "excessive", an interpretation which we do not agree with, and which is not rooted in any language provided within the GDPR. Such an interpretation is overly onerous for data controllers, and not in line with the principle of proportionality set out in Recital 4(2) of GDPR.

The below example demonstrates that a request can be excessive if it produces a very large number of documents for review:

- An employee has sent and received hundreds of thousands of emails during his 19 years of employment with his estate agent employer. When the company searches their email systems and electronic documents for the employee's name and other abbreviations that would identify him, the number of documents initially identified as identifying the employee amount to 300,000 items. For one person to review these emails for the employee's personal data, at the rate of 1,000 emails a day, it would take 1,154 days (just less than four and a half years in working days).

In this case, the request itself is excessive and it would be disproportionate and unreasonable for the estate agents to review to 300,000 emails. The estate agent is a small business and is not expected to hire/outsource the review of the 300,000 documents in order to respond to the request within one month (which would require 15 people working full time). Although the estate agency would be permitted to extend the deadline for compliance by a further two months given the complexity of the request, the request remains excessive and the effort required is disproportionate.

Instead, the employer can ask the employee to clarify the scope of his request. If the employee's clarification does not significantly narrow the request, the employer can take a reasonable and proportionate approach in order to comply with the request by assuming that certain emails will be unlikely to contain personal data (such as emails sent by the employee to clients) and that other emails will be very likely to contain personal data (such as emails sent by the employee to human resources) and are entitled to focus their searches accordingly and proportionately.

- The same scenario as (1) occurs, but for a very small company with limited resources. To comply with the request in its current form will cost so much money that it would bankrupt the small employer. The request is therefore excessive.

- A senior employee (MD role) seeking all data from the entire time period of his employment (6 years +) to date including any email sent mentioning his name, nicknames and employee ID whilst there is ongoing Tribunal litigation. This included WhatsApps from work phones.

- An individual insists on the one month timeframe being adhered to, despite the request involving data spanning many years, requests for clarification being sent to the employee and an explanation being provided as to why this will not be possible.

In this example, it would be helpful if the guidance could clarify if a controller can refuse to comply on the basis of disproportionate effect or motive.

- The time to supply the data is extended by three months, but in order to comply an employer needs to dedicate an individual solely to the task for that period at the detriment of other work.

Manifestly Unfounded Requests

- A former employee who has a history of sending abusive and harassing e-mails to senior management / HR at the former employer in the context of unfounded demands for compensation, who is clearly submitting the SAR with the motive of causing further nuisance for the employer rather than seeking information about the personal data the employer processes.
- It is common in the employment context, for a SAR to be submitted as a negotiation tactic in settlement discussions. An employee will often offer to withdraw their DSAR if the employer accedes to their settlement demands. However that discussion is likely to be subject to without prejudice privilege. The guidance should clarify whether statements made that are subject to without prejudice privilege can be relied on by employers to determine a SAR is manifestly unfounded.

Q5 On a scale of 1 to 5 how useful is the draft guidance?

3

Q6 Why have you given this score

It would be helpful if the guidance included more practical examples that would be relevant for organisations. It would also be useful if the guidance was expressed in a clearer and more succinct manner.

Q 7 To what extent do you agree that the draft guidance is clear and easy to understand?

It is fairly easy to understand but more detailed information and examples as set out above, would be helpful. It would be useful to link the further guidance signposts within the text (to documents, accountability and governance, and data protection by design and default) rather than at the end, as it risks getting lost – the detail in the linked pages is helpful and should be highlighted more prominently.

Q8 Please provide any further comments or suggestions you may have about the draft guidance

- We'd suggest an FAQ section at the end of each section with, say, 5 practical FAQs.
- We recognise that if the guidance were expanded to deal with some or all of these points, it would considerably increase the length of the guidance. Therefore, we would suggest that there could be two sets of guidance, with one specifically aimed

at DSARs made by employees where, as we hope we have demonstrated, the issues in play can be complex.

- **Enforcement**: the guidance refers in its enforcement section to compensation and damages being "if an individual suffers damage or distress". We suggest that the wording is clarified in the light of the Court of Appeal's judgement in *Lloyd v Google LLC [2019] EWCA Civ 1599*, which held that damages can, in principle, be awarded even if there is no financial loss or distress.

ELA Working Party

[redacted] Bryan Cave Leighton Paisner LLP
[redacted] Curzon Green
[redacted] Covington & Burling LLP
[redacted] Simmons & Simmons LLP
[redacted] Glasgow City Council
[redacted] Public Sector
[redacted] Doyle Clayton
[redacted] Lewis Silkin LLP
[redacted] Birmingham City Council
[redacted] GQ|Littler
[redacted] Baker McKenzie – **Co-Chair**
[redacted] Furley Page LLP
[redacted] DAC Beachcroft LLP
[redacted] Norton Rose Fulbright LLP – **Co-Chair**
[redacted] Morgan, Lewis & Bockius UK LLP
[redacted] Legal Advice Centre, University of Law