EMPLOYMENT
LAWYERS
ASSOCIATION

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

ELA L&P Committee: Information Commissioner's Office Employment Practices Call for Views

Response from the Employment Lawyers Association

19 October 2021

ELA L&P Committee: Information Commissioner's Office

Employment Practices Call for Views

Response from the Employment Lawyers Association

19 October 2021

INTRODUCTION

1. The Employment Lawyers Association (**ELA**) is an unaffiliated and non-political group of specialists in the field of employment law. We are made up of about 6,000 lawyers who practice in the field of employment law. We include those who represent Claimants and Respondents/Defendants in the Courts and Employment Tribunals and who advise both employees and employers. ELA's role is not to comment on the political merits or otherwise of proposed legislation or calls for evidence. We 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 and regulation or calls for evidence.

2. A Working Party Co-Chaired by Anna Dannreuther of Field Court Chambers and Clare Fletcher of Slaughter and May was set up by the Legislative and Policy Committee of ELA to respond to the Information Commissioner's Office (**ICO**) Call for Views on Employment Practices (**the Call for Views**). Members of the Working Party are listed at the end of this paper.

3. The Working Party's responses below are drawn from its members' experiences as business owners and as legal advisers to business owners and individuals. The Working Party has responded to questions where the answers are within its area of expertise (either directly or working with clients, or as active and informed members of the legal profession). It has not responded to or commented on questions outside its areas of expertise.

4. In responding, the Working Party has sought to reflect the diverse views and experiences of ELA members. To ensure all views are represented, the Working Party has engaged in independent research where necessary, informed by the members' own legal experience and knowledge of employment law. Any references in this paper to the views of ELA are intended to be inclusive of the views of the minority as well as the majority of ELA members. Whilst not exhaustive of every possible viewpoint of every ELA member on the matters dealt with in this paper, the members of the Working Party have striven to reflect in a proportionate manner the diverse views of ELA's membership.

5. The Working Party has provided this written submission in response to the ICO's Call for Views because, given the large number of comments the group has, it is easier to read in this format. However, in case it is easier for the ICO to process, the

working party has also fitted these answers into the Word format of the Call for Views form. Should the ICO's staff have any questions, please do not hesitate to contact us on LandPChair@elaweb.org.uk.

EXECUTIVE SUMMARY

6. In the nearly ten years since the Employment Practices Code (**the 2011 Code**) was published, there have been multiple, significant changes in data protection law. Most notably, these are:

   6.1 The entry into force of the EU General Data Protection Regulation (**GDPR**) on 25 May 2018 (being adopted from May 2016). This increased sanctions for non-compliance with data protection laws, and sought to harmonise EU laws on data protection;

   6.2 The entry into force of the Data Protection Act 2018 (**DPA 2018**) on 25 May 2018. This Act supplemented the GDPR;

   6.3 The UK's withdrawal from the European Union, with the transitional period ending on 31 December 2020;

   6.4 The retaining of EU data protection law by virtue of sections 2 – 4 of the European Union (Withdrawal) Act 2018;

   6.5 The amending of the DPA 2018 and GDPR by the Data Protection, Privacy and Electronic Communications (Amendments Etc) (EU Exit) Regulations 2019, to create the **UK GDPR** (i.e. the GDPR as amended by post-Brexit UK statutory instruments).

7. Changes in data protection laws have also come about through case law from:

   7.1 The European Court of Human Rights;

   7.2 The Court of Justice of the European Union; and

   7.3 The appellate and first-instance courts and tribunals of the United Kingdom.

8. As will be seen throughout this response, significant cultural and technological changes have also occurred during that ten year period. The way in which employers process the data of their workers has developed in new and increasingly sophisticated ways. When combined with the legal changes outlined above, the need for refreshed guidance from the ICO is clear and compelling. As such, ELA welcomes the opportunity to respond to this Call for Views.

9. There are a number of consistent themes throughout this response, where the need for guidance on data protection in an employment context is perhaps greatest. These include:

9.1 **Consent in an employment context**: The 2011 Code reflects the ICO's position that consent in an employment context is generally not considered to be freely given, in light of the inherent imbalance of power between employers and employees. This causes significant issues in practice, including in scenarios such as criminal records checks, equal opportunities monitoring, and the processing of unstructured data (as explored in more detail throughout this response). This has led to a lack of clarity amongst both employers and employees as to the circumstances in which consent may be validly utilised as a basis for processing employee data. On top of that, the 2011 Code does not yet reflect the new regime for consent under the DPA 2018 and UK GDPR.

9.2 **Special category data**: the nature of an employment relationship is such that it will almost always involve the processing of special category data. Traditionally this has centered on health data (which is reflected in the structure of the 2011 Code). However, our members are increasingly observing other types of special category data being processed, more frequently, and in new ways. The 2011 Code has not kept up with the pace of change in this respect, leaving employers and employees feeling exposed in what is always a sensitive area.

9.3 **Data subject access requests** (**SARs**): While the right to make a SAR is clearly an important right for workers, this can also create an administrative burden for employers. In the experience of some of our members who regularly represent employers, SARs are sometimes used as a pre-litigation tactic by workers who intend to bring claims against their employer. Employers would benefit from a greater understanding of the options available to clarify the scope of a SAR, to request (while not insisting) that the subject narrows their request, or to refuse to act on the request, when the circumstances are appropriate. However, on the other hand, many of our members who represent employees consider that the SAR is a very important right that gives an employee a better chance to understand reasons for their treatment. Our members would therefore find it very helpful if the new guidance could recognise these issues and provide further guidance, to benefit both employers and workers.

9.4 **More technology, more data**: The marked increase in employers' use of technology in recent years has led to a commensurate increase in the amount of employee data they are processing. Innovations such as artificial intelligence (**AI**) and automated decision-making (**ADM**) are fast becoming commonplace in the workplace. The pace of change has accelerated due to the COVID-19 pandemic, with more flexible and hybrid working patterns in some cases being accompanied by more sophisticated employee monitoring and surveillance.

9.5 **International data transfers**: The changing landscape of data protection law precipitated by Brexit has had important implications for how data can

be transferred between the UK and other countries. At the same time, the need for cross-border data transfers in an employment context has only increased, in particular in relation to outsourcing, M&A activity and international recruitment. The 2011 Code needs updating to keep pace with these developments.

10. There are also numerous issues which are specific to the four subject areas currently covered by the 2011 Code. We have elaborated on all of these, along with the overarching themes noted above, in the response below.

QUESTION 1

WE ARE CONSIDERING USING THE CONTENT OF OUR EXISTING GUIDANCE 'THE EMPLOYMENT PRACTICES CODE' AS THE BASIS ON WHICH TO PRODUCE UPDATED GUIDANCE ON DATA PROTECTION ISSUES IN EMPLOYMENT PRACTICES.

WE ARE PROPOSING TO CREATE EMPLOYMENT PRACTICES GUIDANCE TO ADDRESS CHANGES IN DATA PROTECTION LEGISLATION AND THE IMPLICATIONS FOR EMPLOYMENT PRACTICES, INCLUDING DEVELOPMENTS IN RELEVANT CASE LAW. WE THINK THAT THE NEW GUIDANCE SHOULD RETAIN THE FOLLOWING TOPIC AREAS FROM THE CODE:

- **RECRUITMENT, SELECTION AND VERIFICATION**
- **EMPLOYMENT RECORDS**
- **MONITORING AT WORK**
- **INFORMATION ABOUT WORKERS' HEALTH**

WE ALSO PROPOSE TO PROVIDE OTHER SUPPORT AND RESOURCES (INCLUDING UPDATED DATA PROTECTION AND TUPE GUIDANCE).

DO YOU AGREE WITH THE PROPOSED APPROACH?

11. We agree it is sensible to use the content of the 2011 Code as the basis on which to produce updated guidance on data protection issues in employment practices.

12. However, as pointed out throughout this response, data protection law has undergone substantial changes since the 2011 Code and, as such, the content of the sections may vary considerably. There are a considerable number of new areas to address, including the increasing internationalism of employees, new working / recruiting structures, and new attitudes towards personal data (including 'bringing one's whole self to work'). These will all impact on the content of the forthcoming guidance.

Question 3

DO YOU HAVE ANY SUGGESTIONS ABOUT WHAT TOPIC AREAS THE GUIDANCE SHOULD COVER AND WHAT AREAS IN PARTICULAR WE SHOULD FOCUS ON?

13. We elaborate in question 4 below on how the existing sections should be updated in light of cultural and legal changes since the 2011 Code. In this section, we list some further topic areas where we think that employers and workers would benefit from guidance. These are areas that routinely emerge as difficult to navigate, and on which guidance from the ICO would be extremely beneficial:

13.1 **DEFINITIONAL ISSUES:** It would be useful if there could be more guidance on the use of consent in an employment context, as well as other topics such as the distinction between controllers and processors. This could be by including references to other guidance where appropriate, although where there are additional points to be made which are specific and relevant to employment, they should be made in the employment guidance.

13.2 **UPDATED TUPE GUIDANCE:** We welcome the suggestion of updated data protection and TUPE guidance. We would also suggest that guidance would be useful on other forms of data sharing on outsourcings and transitional services agreements where TUPE is not engaged.

13.3 **SPECIAL CATEGORY DATA AND 'HEALTH' SECTION:** We suggest that more guidance is provided on the use of special category data in general (including, but not limited to, health). For example, we have noticed an increased collection and use of data revealing racial or ethnic origin, religious or philosophical beliefs and data concerning a natural person's sexual orientation for the purposes of equal opportunities initiatives and diversity monitoring. Sometimes this is in the specific context of an employer's legal or regulatory obligations (i.e., in the legal industry, and the public sector more broadly, employers are required to publish diversity data) and at other times in the more general context of ensuring diversity in recruitment, planning, training and conference opportunities, pay and promotions. There is also growing evidence that the Equality and Human Rights Commission expects employers to encourage employees to provide diversity data in order to enable more effective equality monitoring (see for example the recent legal agreement between that entity and Jaguar Land Rover which contains such a commitment). We recommend that the ICO considers whether to adapt the "Worker's Health" section of the 2011 Code to cover "Special Category Data", and to provide more guidance on the data protection implications of collating, processing and publicising diversity data, including where this is not done on an anonymised basis.

13.4 **SPECIAL CATEGORY DATA AND CONSENT:** Some employers are seeking to store special category data on an individualised basis (subject to appropriate security measures and access controls) so that employers can ensure diversity in all areas of the business (e.g., project teams). Further

clarification as to the ICO's approach to the use of personal data in that context would be welcome. In particular, guidance on employers' reliance on consent to use special category data (Art 6(1)(a) and Art 9(2)(a) of the UK GDPR), or on legitimate interests (Art 6(1)(f) UK GDPR) and the equality of opportunity condition (paragraph 8, Part 2, Schedule 1 to the DPA 2018), would be helpful.

13.5 **ANONYMISED HEALTH DATA:** Further information on how employers should approach the issue of collecting health data (or equality data) on an anonymised basis (and how to treat such information) will also be useful. For example, we have received questions from employers who have collected data (e.g., for equal opportunity initiatives) on an anonymous basis and who have then sought to use such data in a manner that may mean data subjects are identifiable. Employers would appreciate guidance on this scenario.

13.6 **SARs**: We suggest that employers and workers would benefit from more guidance on SARs in the employment context, as explored in more detail in this response.

13.7 **ENFORCEMENT**: We would also suggest including guidance in respect of the ICO's approach to enforcement, and the consequences of breaches of data protection legislation. Some employers, particularly small companies, are unaware of the extent of their obligations and of the repercussions of a failure to comply with the legislation. Guidance for workers on individual liability for breaches of data protection legislation would also be welcomed.

QUESTION 4

WHAT CHANGES TO DATA PROTECTION LAW SINCE WE PUBLISHED OUR EMPLOYMENT PRACTICES CODE DO YOU THINK WE SHOULD FOCUS ON IN THE EMPLOYMENT PRACTICES GUIDANCE? PLEASE PROVIDE YOUR ANSWERS IN RELATION TO EACH OF THE FOLLOWING TOPIC AREAS:

4A) RECRUITMENT, SELECTION AND VERIFICATION

14. The comments below are provided in the context of:

14.1 Recruitment, by which we mean the sourcing of, and receiving applications from, new potential job applicants;

14.2 Selection, by which we mean the assessment of new job applicants and of current employees in respect of internal vacancies; and

14.3 Verification, by which we mean the screening of applicants after an initial recruitment decision is taken, such as the verification of previous employment, education, pre-employment health checks, and the processing

of DBS and other regulatory checks, to determine overall suitability for employment.

15. We consider that the introduction of the GDPR (now UK GDPR) should be the starting point for the new employment practices guidance. More specifically, there are difficulties when data protection and regulation and other legislation applicable to recruitment, selection and verification don't align fully. We recommend that the ICO carries out an analysis of the intersectionality of data protection law, and other applicable laws, so that the new guidance can acknowledge the tension and provide a practical and realistic route through conflicts that now exist between the UK GDPR and other regulatory frameworks. A simple example is consent in the context of criminal records checks as we demonstrate below:

15.1 **CONSENT NOT FREELY GIVEN IN EMPLOYMENT:** In the context of verification, criminal offences data can be processed under the DPA 2018, Schedule 1, Part 3, Paragraph 29 if the data subject has given consent to the processing. However, there are difficulties in the employment context with relying upon consent. Consent in an employment context is generally not considered to be "freely given" in light of the inherent imbalance of power between employers and employees.

15.2 **EXCEPTION TO THE REQUIREMENT OF CONSENT:** The DPA 2018, Schedule 1, Part 2, Paragraph 12 provides an alternative basis upon which an employer may theoretically rely – that a data controller may process criminal record information in order to comply with a regulatory requirement to identify whether a person (such as a job applicant) has committed an unlawful act or been involved in dishonesty, malpractice or improper conduct. However, the controller may only rely on this condition if the controller cannot reasonably be expected to obtain the consent of the data subject to the processing.

15.3 **BUT CONSENT IS REQUIRED IN AN EMPLOYMENT CONTEXT:** The Rehabilitation of Offenders Act 1974 (**ROA**) expressly requires the consent of the relevant individual before a Disclosure & Barring Service (**DBS**) check is undertaken. It will always be open for the controller to obtain the consent of the data subject to the processing, since consent is a necessary part of the procedure to make a DBS check. The practical result is that it is not possible to satisfy the lawful condition for processing criminal record information under UK domestic law in order to carry out a criminal record check to comply with a regulatory requirement.

15.4 Accordingly, there are difficulties in the employment context of consent being “freely given” therefore consent cannot be a reliable basis for processing and, in the context of an employment or recruitment relationship requiring a DBS, no other avenues appear to be open.

15.5 In practice, employers often undertake different types of DBS checks depending on the role being recruited and the restrictions set out in the ROA (e.g. DBS checks that would show only unspent convictions or DBS checks where spent convictions are shown). It would be helpful for the guidance to address in more detail how employers should deal with undertaking those checks.

15.6 Guidance should provide a way through the tension between the requirement for the controller not to reasonably expect to obtain the consent, yet consent being a necessary part of obtaining a DBS check, as well as provide additional guidance on the circumstances in which it is legitimate for employers to know whether applicants have a criminal record.

16. The exit of the UK from the EEA and the removal of the Privacy Shield scheme as a result of the *Schrems II* decision have implications even if the employer or prospective employer does not have a global workforce. For example, this may be relevant to employers and prospective employers engaging with third party providers located outside of the UK, or that use technology platforms as part of the recruitment process that host or process data in a different jurisdiction (especially in the US).

4B) EMPLOYMENT RECORDS

17. As with other parts of the 2011 Code, the Employment Records section needs updating in light of UK GDPR and the DPA 2018, in particular as regards when consent is appropriate in the employment relationship, the detail of the right to subject access, and references to 'sensitive personal data' (now special category data), including reference to the extra bases and additional safeguards for processing such data, as well as appropriate policy documents and additional safeguards.

18. We have set out below some specific examples of how we think the sections in the existing 2011 Code should be updated:

18.1 **SECURITY**: This section should take account of the decision in *WM Morrison Supermarkets plc v Various Claimants* [2020] UKSC 12, [2020] AC 989, and provide employers with guidance about what steps they should take to limit their liability under both the DPA 2018 and under common law vicarious liability principles.

18.2 **PENSION AND INSURANCE RECORDS**: This section should refer to the distinction between controller-processor (which require Article 28-compliant agreements) and controller-controller relationships (which do not). It would also be helpful if the ICO provide guidance on what it considers fall into each categories.

18.3 **EQUAL OPPORTUNITIES MONITORING**: It would be helpful if the guidance referred to the appropriate legal base/bases for this processing. The guidance also needs to be updated to refer to the specific substantial public interest exemptions in the DPA 2018.

18.4 **MARKETING**: This section refers to a positive "opt-in" requirement but does not refer to the "soft opt-in".

18.5 **WORKERS' ACCESS TO INFORMATION ABOUT THEMSELVES:** This section of the 2011 Code contains a lot of information which is already in the ICOS's updated SARs guidance (https://ico.org.uk/right-of-access). We suggest that the ICO should consider using more cross references to that SARs guidance, albeit that guidance which is specifically relevant to employment should be retained and restated here. In terms of other updates:

(A) The section of the 2011 Code in relation to the timescales for delivering a response to a SAR requires updating. Under Article 12(3) of the UK GDPR, an organisation will need to respond to a SAR without "undue delay" and in any event within one month of the request, unless an extension can be justified.

(B) The 2011 Code should be updated to clarify the identification required when a SAR is made. Article 12(6) of the UK GDPR requires that only information "necessary" to confirm the identity of the data subject should be requested by the employer, where there are doubts regarding identity. We suggest that wording to this effect should be included in the guidance to deter employers from creating onerous or prohibitive identification requirements which could discourage individuals from making SARs.

(C) The 2011 Code should be updated to clarify that the UK GDPR does not require or encourage the provision of information in a hard copy form. If the request was made originally by electronic means, information should be provided "in a commonly used" electronic form unless otherwise requested by the employee (Article 15(3), UK GDPR). In our experience, SARs are predominantly being provided electronically, and UK GDPR would therefore require the response to also be provided electronically. The guidance should be updated to reflect this.

(D) The 2011 Code needs updating to alert employers to the information that must be given under Article 13 of the UK GDPR relating to, inter alia, the purpose of data processing, the recipients of personal data and the storage of the data. The guidance should make clear that the employer must provide this irrespective of whether the subject has requested it or not.

18.6 **REFERENCES**: The guidance requires updating to clarify that confidential references are exempt from disclosure and therefore do not fall within the right of access for a subject. It also requires updating to reflect that the exemption now covers employment references both given and received (not just those given, as under the DPA 1998). It would also be beneficial for the guidance to include mention of references also received in respect of prospective employees, which data controller obligations will also extend to.

18.7 **DISCLOSURE REQUESTS**: The guidance will require updating to reflect the correct sources of data protection law and guidance which employers and relevant officers will need to refer to before making disclosure decisions. The guidance should also be updated to refer to the relevance of "adequacy decisions" and why it is important that employers monitor the position. Employers should still be directed to the ICO guidance to assist with this aspect as it continues to evolve.

18.8 **PUBLICATION AND OTHER DISCLOSURES**: The guidance should be updated to expand on what is meant by "consent". Article 4(11) of the UK GDPR requires consent to be freely given, specific and informed. The guidance should emphasise this to employers to deter them from relying upon passive forms of consent, such as the mere signing of prescribed forms. It would be helpful for the guidance to include modern references of what publications employers are likely to encounter. For example, the guidance could reference staff photos on a website, or information published on social media, to ensure employers understand the remits of publication.

18.9 **MERGER, ACQUISITION AND BUSINESS RE-ORGANISATION**: It would be helpful if the guidance referred to the appropriate legal base/bases for this processing and any applicable exceptions (e.g. from needing to provide data subjects with information that their data is being shared in certain ways, such as where insider trading might be a concern or information sharing might affect share prices). In addition, references to international transfers need updating in light of the changes in the law for transferring data.

18.10 **DISCIPLINE, GRIEVANCE AND DISMISSAL**: References to the Data Protection Act 1998 need updating. It would also be useful if the guidance considered the position for trade union representatives who act as representatives for workers and joint data controllers under Article 26 UK GDPR.

18.11 **OUTSOURCING DATA PROCESSING**: This section needs updating in light of (i) the changes in the rules for transferring data to processors and the contractual requirements for that relationship; (ii) the changes in the rules for transferring data internationally; and (iii) in respect of its security references i.e. BS7799.

18.12 **Retention of records**: References to the Data Protection Act 1998 need updating. Reference to the right of erasure under Article 17 of the UK GDPR should also be included. Employers should be aware of how to deal with requests from employees who validly exercise this right.

4C) MONITORING AT WORK

19. Monitoring and associated data privacy rights have undergone major changes since the publication of the 2011 Code.

20. When the 2011 Code was released (and its supplementary guidance) the main piece of legislation around monitoring was the Data Protection Act 1998 (**DPA 1998**). The 2011 Code also references the Regulation of Investigatory Powers Act 2000 (**RIPA 2000**).

21. The law has significantly developed from the above two Acts, as outlined below. The two most relevant pieces of legislation now are:

    21.1 the DPA 2018;

    21.2 the UK GDPR; and

    21.3 The Investigatory Powers Act 2016 (**IPA 2016**), which has also replaced the RIPA 2000.

22. This section of the response focuses on the relevant parts of the 2011 Code, Supplementary Guidance (**the Supplementary Guidance**) and Quick Guide (**the Quick Guide**) relating to monitoring, namely:

    22.1 pages 58 – 77 of the 2011 Code;

    22.2 pages 45 – 62 of the Supplementary Guidance; and

    22.3 pages 13 – 17 of the Quick Guide.

23. The relevant changes are outlined below, in addition to highlighting some parts of the 2011 Code, Supplementary Guidance and Quick Guide which are now updated.

DATA PROTECTION OFFICERS

24. Data Protection Officers (**DPOs**) were not required under the DPA 1998. Unsurprisingly, the 2011 Code (and Supplementary Guidance and Quick Guide) therefore make no reference DPOs.

25. Monitoring is a contentious topic, with various data privacy implications. We would therefore expect, as a best practice, DPOs (where one is appointed) to be

consulted around any proposed monitoring to review the potential impact on individuals and the against the legitimate aims pursued by the employer.

26. While not all organisations require a DPO (see Article 37(1) UK GDPR and the ICO's own resources which could be cross referred to in the new guidance - https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-officers/), even where an employer is not required to appoint a DPO, the ICO's own guidance (referenced in this paragraph) suggests data privacy should still be assigned to someone within the organisation, since the guidance states organisations "*must ensure that [they have] sufficient staff and resources to discharge [their] obligations under the UK GDPR*".

27. We recommend clear references should be made throughout the new guidance to who needs to be consulted, namely the DPO if the employer has one, and if not the relevant senior members of management responsible for data privacy. The consultations should be held with the project managers leading any monitoring proposal or senior managers sponsoring the proposal.

28. The 2011 Code (at page 65) suggests as good practice employers should: "Identify who within the organisation can authorise the monitoring of workers and ensure they are aware of the employer's responsibilities under the Act." We suggest adding wording here around the use of DPOs, or at the very least, cross refer back to other ICO guidance on when a DPO is required.

CONSENT

29. The UK GDPR and DPA 2018 significantly raise the hurdle for consent (as defined in Article 4(11) of the UK GDPR). In an employment context, the ICO's own guidance and provisions of the UK GDPR show why consent is difficult to rely on.

30. The biggest hurdle for employers relying on consent as a lawful ground for processing is showing that consent from an employee is "*freely given*". The ICO notes the imbalance in bargaining power between employers and employees.[1]

31. Further, if any special category data is concerned, the UK GDPR requires the consent to be explicit (Article 9(2)(a) UK GDPR). Notwithstanding the significantly reduced contexts in which employee consent can be relied on as a lawful ground for processing compared to the position under the DPA 1998, reference should be made to the distinction between consent and explicit consent. We, of course, note the ICO's own position that due to the higher hurdles for consent under the UK GDPR, explicit consent is unlikely to be very different from the usual standard of

[1] See: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/when-is-consent-appropriate/

consent (https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/#ib4).

32. At this point, it is also worth noting that other Supervisory Authorities have fined employers for incorrectly relying on consent. For example, in July 2019, the Hellenic Authorities fined PWC €150,000 for incorrect use of consent as a purported lawful ground for processing under the GPDR (https://edpb.europa.eu/sites/default/files/files/news/summary_of_decision_26_2019_en_2.pdf). This fine concerned various types of processing, but monitoring is clearly one of the more intrusive means of processing areas.

33. The 2011 Code (at page 62) references obtaining the employee's consent. While the response outlining the problems with relying on consent is still the correct starting point, with the additional difficulties found under the UK GDPR, this approach seems outdated and we recommend it is amended to further emphasise the novel difficulties in relying on consent.

SPECIAL CATEGORY DATA

34. The UK GDPR and DPA 2018 changed the categories of personal data. "Sensitive personal data" under the DPA 1998 is now known as special category data.

35. Special category data is wider than the previous definition of sensitive personal data since it expressly includes biometric and genetic information. It also includes trade union membership. Some monitoring systems used by employers might use biometric information, for example if fingerprints are used to gain access to a premises, as is sometimes seen at workplaces and sites where security is important, such as hotels, or for staff to register the time they start their shift and finish their shift. New guidance for how employers may be able to utilise such technology and how this impacts any potential monitoring for this type of information will again be welcome.

36. Depending on the type of monitoring, special category data could be involved. In addition to the example above on biometric data, in any video surveillance a controller could be processing information on race. Highlighting this issue, and indicating how it should be addressed by controllers and alerting them to the potential lawful grounds to processing under Articles 6 and 9 UK GDPR is recommended.

FURTHER CONSIDERATIONS FOR SPECIAL CATEGORY DATA – APPROPRIATE POLICY DOCUMENT AND ADDITIONAL SAFEGUARDS

37. The DPA 2018 requires data controllers to have an appropriate policy document (**APD**) if relying on certain conditions for processing special category data (as might be the case with monitoring). The data controller must retain the APD and record processing in accordance with Schedule 1 Part 4 paragraphs 38-41.

38. APDs and the additional safeguards outlined below were not required under the DPA 1998, so the 2011 Code has no reference to them. From our experience, this is one of the more often overlooked policies for organisations trying to ensure they have a full suite of policies for the data privacy obligations. The new Code should address this gap in coverage.In the employment context, the most likely applicable sections for monitoring are:

38.1 Schedule 1 Part 1: where processing is necessary for the purposes of performing or exercising obligations or rights imposed or conferred by law on the controller or the data subject in connection with employment.

38.2 Schedule 1 Part 2: where processing is for substantial public interest conditions, which include:

(A) equality of opportunity or treatment;

(B) racial and ethnic diversity at senior levels of organisations;

(C) preventing or detecting unlawful acts;

(D) support for individuals with a particular disability or medical condition;

(E) counselling;

(F) safeguarding of economic well-being of certain individuals;

(G) occupational pensions; and

(H) publication of legal judgments.

38.3 Schedule 1 Part 3: for any employers processing criminal convictions.

39. For criminal records, a separate subsection would help employers when considering their specific lawful basis (such as explicit consent).

40. The APD under Schedule 1 Part 4 DPA 2018 must:

40.1 explain the controller's procedures for securing compliance with the six principles in Article 5 of the UK GDPR;

40.2 explain the controller's retention and erasure procedures for the personal data processed under the relevant condition, and an indication of how long the data is retained;

40.3 be reviewed and updated (if appropriate from time to time);

40.4 be made available to the ICO on request without charge; and

40.5 be maintained from the time processing starts until six months after processing ceases.

41. Further, employers need to maintain a record of processing under Article 30 UK GDPR which contains the following information.

41.1 the condition being relied on under Parts 1, 2 or 3 of Schedule 1 DPA 2018;

41.2 the lawful basis being relied on for the processing in accordance with Article 6 UK GDPR; and

41.3 whether the data are retained and erased in accordance with the appropriate retention/erasure policy and if not, the reasons why the policies are not followed.

42. A section on APDs, including how and when the additional safeguards might apply in practice, would greatly assist data controllers. This might be used in conjunction with the requirement to consider using data protection impact assessments (**DPIAs**) to be carried out in the event of processing likely to result in high risk to the rights and freedoms of individuals under Article 35(1) UK GDPR, for example, where an employer decides to monitor workplace trade union representatives organising industrial action and / or staff who are trade union members and participate in industrial action.

RIGHT TO HAVE INACCURATE INFORMATION CORRECTED

43. Section 3.1.8 of the 2011 Code references the risk of malfunctions causing information to be misleading or inaccurate.

44. Further to a controllers' obligations to keep data accurate and up to date (Article 5(1)(d) UK GDPR), Article 16 UK GDPR gives data subjects the right (not seen in DPA 1998) for data subjects to:

44.1 correct inaccurate personal data held by the controller; and

44.2 complete incomplete personal data held by the controller.

45. A separate section on data subjects' rights to have their information corrected, including where inaccurate information is processed due to a malfunction in monitoring software, should be included.

PRIVACY NOTICES

46. Data subjects have the right to know what personal data is processed on them and further information under Article 13 UK GDPR.

47. A lot of this information is provided through privacy notices. However, for certain types of monitoring, further information may be needed.

48. As the 2011 Code already rightly points out, covert monitoring is almost never justified, save for in very limited circumstances, namely only for the prevention or detection of criminal activity or equivalent malpractice (as noted by the 2011 Code at section 3.4.5). The legal position has not changed on this through DPA 2018 or UK GDPR.

49. We suggest Section 3.2.5 of the 2011 Code should be more comprehensive on methods of notifying data subjects that their information might be monitored, for example through the use of specific information within privacy notices and (for physical means of monitoring, such as CCTV) prominent signage, which could direct individuals to a relevant privacy notice.

AUTOMATED DECISION MAKING (ADM)

50. While we believe the practice is currently uncommon, employers could (especially in the absence of any clear guidance in the 2011 Code, assuming this is their starting point for data privacy considerations) try and use monitoring via ADM to make decisions on their staff. This is especially relevant given the rise of remote working and working from home accelerated by COVID-19.

51. Under the UK GDPR, data subjects have the right not to be subject to ADM, including profiling, which has legal or other significant effects on the data subject (Article 22(1) and Recital 71 UK GDPR). The exceptions to this are when the ADM is:

    51.1 necessary for entering into or performing a contract with the data subject;

    51.2 authorised by EU or member state law applicable to the controller if the law requires suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or

    51.3 based on **explicit** data subject consent (emphasis added).

52. With the high hurdle of consent, especially explicit consent, under the UK GDPR and its limited application to the employment context (due to the imbalance of bargaining power between employers and employees), the very limited potential for ADM for monitoring needs outlining in the updated guidance. For example, even where automated input is made (such as logging times someone scans their biometric information in to access a restricted area / clock on for their shift), in practice we would expect human intervention before any decisions with legal or other significant effects.

IPA 2016

53. The 2011 Code (at page 69) requires employers to "Ensure that where monitoring involves the interception of a communication it is not outlawed by the Regulation of Investigatory Powers Act 2000".

54. The Regulation of Investigatory Powers Act 2000 was replaced by IPA 2016. Most of the relevant data privacy concerns are around the DPA 2018 and UK GDPR. IPA 2016 prohibits interception of communications without lawful authority. The 2011 Code needs updating to refer to IPA 2016.

55. It would be helpful if the guidance also makes reference to the Statutory Instrument The Investigatory Powers (Interception by Businesses etc. for Monitoring and Record-keeping Purposes) Regulations 2018, as this is the most relevant to employers.

4(D) - INFORMATION ABOUT WORKERS' HEALTH

56. The employment practices guidance should focus on key areas impacting the collection and use of personal data under the **UK GDPR** and **DPA 2018**, taking into account European case law and guidance (which, though not binding, remain instructive post Brexit). We outline below the key areas that we, as employment law practitioners, see presenting particular challenges for organisations in the context of collecting and using data concerning the health of their workers.

LAWFUL BASES PROCESSING HEALTH DATA

57. In order to collect and use personal data concerning the health of workers, employers need to identify and record a legal basis for processing under Article 6 of the UK GDPR and a condition for processing health data (as "special category" data) under Article 9 of the UK GDPR and Schedule 1 to the DPA 2018. It is often challenging for employers to identify the appropriate lawful basis for processing workers' health data in the context of different processing activities. It would be helpful to have more tailored guidance on the lawful bases for collection and use of personal data in the employment context. We suggest that the new guidance could expand on (and should be cross-referenced with) the relevant sections of the ICO Guide to the GDPR.

58. The relevant sections of the ICO Guide to the GDPR (or linked "Detailed Guidance") currently provide helpful information (and some examples) on the following lawful bases for processing personal data in the employment context:

    58.1 *Consent (Art 6(1)(a) UK GDPR):* (see existing ICO guidance here). Further guidance on the validity of consent given the employer/worker relationship would be helpful. For example, there may be occasions where consent to the use of health data is appropriate and voluntary (e.g., noting a worker's allergies in the context of a work social event). The new guidance should refer to and expand on the WP29 guidance (see here at paragraph 3.1.1) and the existing ICO guidance referred to above.

58.2 *Necessary for compliance with the employer's legal obligations ((Art 6(1)(c) UK GDPR):* The example given in the existing ICO guidance (here) relates to the provision of employee salary records to HMRC. Additional guidance in relation to legal obligations in the employment context to provide a safe working environment, to comply with the duty to make reasonable adjustments and other aspects of anti-discrimination legislation would be helpful.

58.3 Necessary for the purposes of the legitimate interests pursued by the employer or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data ((Art 6(1)(f) UK GDPR): Employers may seek to rely on the "legitimate interests" basis for many processing activities, for which a (sometimes complex) balancing test is required. The ICO has published detailed guidance on the legitimate interests basis here, including some examples in the employment context. We suggest that the new employment practices guidance should include further information for employers on how to conduct a legitimate interests assessment.

58.4 The new guidance should also provide guidance on assessing whether a DPIA would be necessary in specific uses of health data by employers. This could draw on challenges faced by employees and workers in the context of attending/returning to the workplace during the Covid-19 pandemic and the collection of test results and vaccination status by employers. Notably, employers and workers would benefit from guidance on the collection of health data from third parties, such as workers' dependants, in the context of the administration of employment benefits (such as health insurance) and considering obligations under anti-discrimination laws. It would also be helpful if the guidance could consider the scope of the consultation requirement with employees and their representatives under Article 35(9) UK GDPR.

58.5 We note the consultation issued by the DCMS recently (See https://www.gov.uk/government/consultations/data-a-new-direction). This introduces the concept of a defined list of activities that would be regarded to be in the legitimate interests of the data controller, and for which a balancing test would not be required. This may include processing for employment purposes.

59. The ICO Guide to the UK GDPR does not provide guidance on the following lawful bases for processing under Article 6 of the UK GDPR in the employment context:

59.1 Necessary for the performance of a contract ((Art 6(1)(b) UK GDPR): It would be helpful for the new employment practices guidance to cover when (if ever) this basis could apply to data concerning workers' health. For example, employers and workers may question whether this basis could apply to health data processed in the context of a pre-employment

competency assessment designed to ensure that a worker is able to undertake certain activities intrinsic to the role, where there is no legal obligation to undertake that assessment. Workers may argue that the "legitimate interests" basis should apply, so that any adverse impact on them is taken into account; employers may argue that a particular competency is necessary for the role and that the "performance of a contract" basis should apply.

SPECIAL CONDITION FOR PROCESSING HEALTH DATA

60. In order to process worker health data, an appropriate condition for the processing must be identified under Article 9 of the UK GDPR (as supplemented by Schedule 1 to the DPA 2018). The ICO has published detailed guidance on processing special category data here. Further guidance would be helpful to address the following special conditions for processing in the employment context:

60.1 *Employment, health and safety, social protection (Art 9(2)(b) UK GDPR and paragraph 1, Schedule 1 DPA 2018):* No examples are currently provided in the detailed guidance on processing special category data about the use of health data for Equality Act 2010 (reasonable adjustment) purposes. Further information on the collection of medical data in the context of sickness absence records would also be helpful. We also suggest that the new guidance should cross-refer with the ICO's Covid-19 guidance here and that the ICO considers including a generic section on collection and use of employee health data in connection with public health emergencies (to extend beyond the current pandemic).

60.2 *Explicit consent (Art 9(2)(a) UK GDPR):* It would be helpful if the new employment practices guidance could provide any examples where explicit consent may be appropriate to enable employers to collect and use health data. For example, in the context of data regarding disability status for equality and diversity monitoring where an employer seeks to collect the information on an individual, rather than an aggregated, basis.

60.3 *Substantial public interest (Art 9(2)(g) UK GDPR):* The new employment practices guidance should include more information on the application by employers of the conditions relating to the equality of opportunity and ensuring racial and ethnic diversity in senior management (paragraphs 8 and 9 of Schedule 1 to the DPA 2018).

60.4 We suggest that the new employment practices guidance provide more information on preparing an APD in the context of processing worker health data, the necessity for (or overlap between) the APD and any DPIA that has been carried out for the same processing, and more detail on the additional safeguards under Schedule 1 Part 4 DPA 2018.

TRANSPARENCY – WORKER PRIVACY NOTICES

61. In order to comply with the transparency principle under UK GDPR, employers tend to provide privacy notices to workers: (i) during the recruitment phase; and (ii) as part of the onboarding process about the collection and use of personal data. The privacy notice tends to sit within a Staff Handbook, and is reviewed/updated from time to time. Specific notices may also be given (e.g., as part of a document review exercise in an internal investigation or where data is collected for equal opportunities monitoring purposes). The new guidance could usefully highlight the danger of adopting new or different purposes for processing of data, for example following the introduction of new technologies, monitoring performance/capability etc.

62. The ICO has provided guidance on the specific requirements under Articles 13 and 14 of the UK GDPR (see here). We suggest that the new employment practices guidance should cross refer to the detailed guidance. It would also be helpful if the new guidance included a basic template or "building tool" for employers to use when drafting a privacy notice for workers, in a similar manner that the ICO has done for public privacy notices in its SME hub (see here). This would be particularly useful for small and medium sized organisations who are in many cases spending considerable time and resources navigating the requirement to include numerous provisions in a worker privacy notice whilst ensuring that they convey the information in a clear and transparent way.

CROSS BORDER TRANSFERS

63. Employers would benefit from additional guidance on how to handle cross-border data transfers, particularly in relation to intra-group data transfers and where employers share personal data relating to workers with controllers (including group companies) or processors abroad. As part of the ICO's recent consultation on the new international data transfer agreement and guidance, additional information on how the personal data of workers (in particular, health data) should be assessed when carrying out a transfer risk assessment for such data will be useful.

64. We note that the ICO's draft international transfer risk assessment and tool (see here) at page 21 lists special category records of staff as high risk; however, further information on whether this will lead to an enhanced risk of harm to data subjects in all instances, or whether the likelihood of a third party (such as an overseas surveillance body) accessing such data may be taken into account, will be helpful (i.e., if it could be sufficiently low to justify the transfer).

65. Employers will also benefit from further guidance on whether they may rely on the explicit consent of employees to carry out a cross-border transfer under Article 49 of the UK GDPR. This is particularly relevant to employers who are based in a non-adequate country and who employ their employees through this foreign entity (where they are unable to enter into standard contractual clauses to facilitate the restricted transfers, as no UK-based entity exists). In contrast, we note that Recital

7 of the new EU Standard Contractual Clauses (see here) specifies that the standard contractual clauses may only be used where a data importer is not subject to the GDPR (i.e., excluding foreign entities who are subject to the GDPR). If it is possible for employers to rely on this exemption in certain scenarios, then additional information on the steps that employers should take to demonstrate that such explicit consent is freely given in this context will also be helpful.

QUESTION 5

APART FROM RECENT CHANGES TO DATA PROTECTION LAW, ARE THERE ANY OTHER DEVELOPMENTS THAT ARE HAVING AN IMPACT ON EMPLOYMENT PRACTICES THAT YOU THINK WE SHOULD ADDRESS IN FUTURE EMPLOYMENT PRACTICES GUIDANCE? NON-EXHAUSTIVE EXAMPLES OF SUCH DEVELOPMENTS COULD INCLUDE OTHER LEGAL CHANGES, TECHNOLOGICAL DEVELOPMENTS, CULTURAL CHANGES, AND THE IMPACT OF THE COVID-19 PANDEMIC. PLEASE PROVIDE YOUR ANSWERS IN RELATION TO EACH OF THE FOLLOWING TOPIC AREAS:

5A) RECRUITMENT, SELECTION AND VERIFICATION

66. Employment practices have evolved significantly since the 2011 Code was published. Key developments that ought to be addressed in future employment practices guidance are as follows.

UNSTRUCTURED DATA

66.1 The world of unstructured data is now too large, partially as a result of the sheer volume of emails, video conferencing and messages over platforms such as Microsoft Teams, particularly from last 18 months. By "**unstructured data**" we mean data which is not collected in a deliberate and structured way (such as a new employee questionnaire), but instead is collected through electronic communications between employees or between employees and external third parties (such as emails), often inadvertently or ancillary to business as usual interactions. This has a number of ramifications for employers, prospective employers and recruitment agencies and there needs to be pragmatic guidance on a number of aspects relating to unstructured data in order to assist data controllers. This is explored further in sections 128.1-128.4 below.

DIVERSITY

66.2 In recent years there has been an increased focus upon, and scrutiny of, diversity in the workplace, resulting in increased collection and processing of personal data – particularly special category data which is used within the employer organisation and may also be shared with third parties such as regulators or, in certain circumstances, clients/customers.

66.3 Processing of personal data in this respect is used to (i) monitor the existing make-up of a workplace, (ii) inform decisions and measures to improve diversity and (iii) report externally (to regulators, markets, clients/customers and the public at large) about workplace diversity (for example, the existing gender pay gap reporting obligations and the proposed ethnicity pay gap reporting regime as well as where clients/customers seek information on how diverse their client/customer teams are). Article 9(2) of UK GDPR provides some bases for processing special categories data. It would be helpful for employers to have guidance on the legal basis for processing and how that data should be dealt with. For example, in some cases employees are asked by their employers to share their diversity information (which may include special category data) and can elect whether or not to share the information, but the issue of the validity of employee consent comes up again.

66.4 Some regulated sectors of the economy (such as financial services) are also seeing an increased focus on the collection and processing of certain special categories of personal data from other regulators. In the short to medium term it is possible that employers in such sectors will be subject to regulatory obligations to report on, for example, the gender and ethnic diversity amongst appointees to internal and external vacancies (or in the case of the financial services sector, potentially all protected characteristics under the Equality Act 2010 as well as socio-economic status for those applying for senior manager roles that require regulator approval), in addition to particular groups of existing employees.[2] Such reporting will inevitably lead to an increase in the processing of personal data (including special categories of personal data) where previously there had been a move towards anonymous recruitment.

WORKPLACE AUTHENTICITY

66.5 A related topic is how employers and prospective employers should treat the unstructured but sometimes unavoidable collection of personal data shared by employees and job applicants. Employers are now far more alive to issues of mental health and wellbeing than they were when the 2011 Code was published. In that context, employers have an increased focus on creating a culture of transparency, where employees are encouraged to be their authentic selves in the workplace. This can relate to many aspects of an employee's self, including (purely by way of example) their sexuality, their gender identity or, as increasingly prevalent, their mental health.

66.6 This increasingly translates into employees sharing their personal experiences of, for example, mental health to encourage others to feel

[2] https://www.fca.org.uk/publications/consultation-papers/cp21-24-diversity-inclusion-company-boards-executive-committees

comfortable in the workplace. This can be both informal (in the sense of employees informally sharing their experiences with each other) or formal (with employers recording and sharing on their intranet employees discussing their personal experiences). In the context of recruitment and selection, a job applicant may have published information on social media (such as LinkedIn) concerning their mental health or a current employee may have done so on a company intranet or this information may be published as part of recruitment materials. Applicants may also share much more personal data and special category personal data during interviews than in the past as part of this culture of transparency and bringing your whole self to work.

66.7 As a result, employers or prospective employers could end up holding and processing special category personal data in respect of, for example, employees' health and sexuality. The use of such initiatives to facilitate increased wellbeing in the workforce is to be welcomed, but the mishandling of such data can inadvertently lead to actual or perceived bias in the recruitment or selection process. It would be helpful for employers to have guidance on the legal basis for processing this type of data, and how to lawfully process this data (including duration of storage).

ROLE OF THIRD-PARTIES IN THE RECRUITMENT PROCESS

66.8 The recruitment process is increasingly outsourced by employers or prospective employers to, for example, recruiters to source suitable candidates or third parties to conduct initial screening of potential candidates. Such out-sourcing necessarily involves the sharing of personal data between the prospective employer and the third party.

66.9 Recruitment is also increasingly dependent upon the use of social media, particularly sites such as LinkedIn as well as Google searches, with employers or recruiters often relying upon information publicly available on social media or the Internet to (i) source and (ii) vet potential candidates. This necessarily involves the collation and processing of candidates' personal data from publicly available information, sometimes necessarily before there has been any contact between the individual and the organisation. There could be implications for data subjects' rights to privacy, and clarification on this increasingly common practice would be welcome.

REMOTE RECRUITMENT

66.10 COVID-19 has seen a surge in the use of technology in the sourcing and assessment of candidates. This includes, for example, the use of video-conferencing platforms such as Microsoft Teams and Zoom to conduct video interviews.

66.11 Many candidates want to maximise their employment opportunities and are prepared to do video interviews that can be recycled, either by one employer or shared with a number of prospective employers. Our understanding is that this is a relatively new way of working within the recruitment industry.

66.12 Such mechanisms invariably give rise to the processing and retention of personal data in a way that potentially would not be quite so easily identified in a search triggered by the exercise of rights by a data subject. In addition, there may be inadvertent processing of special category personal data if this can be inferred from images and/or the contents of such video interviews.

COVID-19 AND VACCINATIONS

66.13 Post-COVID-19 there may be a desire – and in some sectors (such as healthcare) a requirement – on the part of employers and prospective employers to understand the vaccination status of their workforce and/or job applicants, even where there is no legal obligation on employers to collect such data. In addition, information may well be processed by an employer or potential employer in relation to whether the individual, if they have not been vaccinated, has recently had a negative COVID-19 test or had COVID-19 in the recent past such that they are likely to have immunity.

66.14 Where relevant, prospective employers (or recruitment agencies on behalf of their clients) are likely to collect and process health related personal data (i.e. in respect of vaccination status) at the recruitment stage, in quantities that would not previously have been seen in the recruitment process outside of the duty to make reasonable adjustments. In certain sectors, such as healthcare, such data may be used to inform recruitment decisions; i.e. employment may only be offered to those who have been vaccinated.

ADM/USE OF AI IN RECRUITMENT

66.15 The use of technology during the recruitment process which involves ADM is far more common than when the 2011 Code was written. Employers would benefit from the guidance covering this topic in some detail; to help them understand how and when they can use ADM, what information should be shared with a candidate about the use of ADM and the candidate's rights to challenge a decision and have human intervention. This is a topic that is likely to grow in significance in the future.

INTERNATIONAL RECRUITMENT

66.16 For some employers the recruitment market is much more international now than when the 2011 Code was first published. As a result, there is a greater flow of personal data about candidates and more data arising from the

recruitment process that crosses borders. For example, a candidate may be based in the UK but work for an Australian company with data being transferred to Australia or a candidate may be based in France but recruited to work for a UK company. Guidance on how employers should deal with these types of data transfer would be helpful.

5B) EMPLOYMENT RECORDS

67. We agree that the 2011 Code as a whole should be updated to reflect technological developments, cultural changes, and the impact of the Covid-19 pandemic. We have set out below specific examples of how we think certain sections of the Employment Records part of the 2011 Code should be updated.

68. **INTRODUCTION**: under 'What does this part of the code cover?', there is a reference to some subsections of the 2011 Code only likely being of relevance to larger organisations, without any indication of which subsections these are. It would be helpful if the new guidance could be more explicit if different guidance or standards are applied to employers based on their size (or other factors, such as their sector or activities). Similarly under 'Sickness and injury records', the 2011 Code states that "*Employers are advised as far as practicable to restrict their record keeping to absence records rather than sickness or injury records*." This is unlikely to be workable for most employers, given the existence of other legal obligations under employment and health and safety legislation, for which the nature of the worker's sickness or injury, not simply the fact of their absence, will be relevant.

69. **SECURITY:** This section should be updated to reflect the implications of more widespread remote and hybrid working patterns on the security of employment records.

70. **PENSION AND INSURANCE RECORDS**:

    70.1 This section assumes that pension or insurance schemes are often managed by employers in house. We do not consider that this assumption should be made, and the guidance should also address the situation where the schemes are managed by a third party.

    70.2 This section should also take into account the technological advancements in methods of data sharing (the current guidance refers to "sealed envelopes") and security mechanisms that employers could use, such as encryption/password protection.

    70.3 In practice, we consider that it is unusual that employers will collect data to share with third parties that they will not otherwise need to retain themselves. Quite often medical providers will also obtain information directly from employees.

71. **EQUAL OPPORTUNITIES MONITORING:** The guidance should acknowledge that equal opportunities monitoring is becoming increasingly common in the employment context. We consider that the guidance should give a stronger view on ensuring anonymity given the sensitivity of data and explain the circumstances in which equal opportunities data can be revealed (and in particular, whether consent is appropriate).

72. **MARKETING**: In our experience, it is unusual for employers actively to market to their employees. Nonetheless, it would be helpful for the guidance to acknowledge that often employees' data is transferred to third party benefits providers, as should be set out in the employer's privacy notice. Once the third party has obtained that data and once the employee and third party have a direct relationship, it is possible that the third party may market directly to the employee, although this is a matter for the third party and the employer.

73. WORKERS' ACCESS TO INFORMATION ABOUT THEMSELVES:

73.1 Due to technological developments, online messaging platforms have become a broad and sizeable element of data potentially caught by SARs. The guidance should address how employers can manage this in practice.

73.2 In our experience, employers would find it helpful to have guidance on their ability to clarify the scope of a SAR, as well as their ability to ask the subject to provide additional details about the information they want to receive, such as the context in which the employer may have processed their information and the likely dates of when the employer processed it. The guidance should make it clear that employers may ask the data subject to narrow their request (for example if their request is vague or likely to contain a significant amount of data which is neither useful or substantive), but that the data subject cannot be forced to narrow their request. Creating further dialogue between the data subject and the employer is likely to improve the efficiency and speed of compliance with the request.

73.3 Similarly, employers should be advised of their right to refuse to comply with a SAR, or to charge a fee for complying, if the request is considered manifestly unfounded or excessive.

73.4 If employers are intending to provide results by electronic means, employers should still be reminded of the need to transfer data securely (and of employees' rights under Articles 21 and 22 UK GDPR), particularly given the increased use of home working.

74. **REFERENCES AND DISCLOSURE REQUESTS**

74.1 Due to the international nature of many companies, more guidance on the appropriate sharing of information between offices/ departments would be helpful.

74.2 The implications of Brexit has already created a changing landscape for data protection law in general, but more specifically how data can be transferred between other countries. Employers will need to be increasingly mindful of this, particularly those with workers in different countries. The guidance should include reference to relevant ICO sources where current information can be found on transfers of data specifically.

75. PUBLICATION AND OTHER DISCLOSURES

75.1 Due to technological developments, images and information are shared more commonly and more freely by employers on websites and social media pages. It would be helpful for the guidance to consider how the "right to be forgotten" could impact business and marketing materials and have mechanisms to either remove images or information, or otherwise have an ongoing, lawful basis for processing the data.

75.2 As above, the current meaning of "consent" should be clarified in the guidance.

76. MERGER, ACQUISITION AND BUSINESS RE-ORGANISATION

76.1 Most mergers and acquisitions now require documents to be uploaded and accessed via a data room. This data room might have documents uploaded in one country, being hosted in another country, with the data room company being based in a third country and the data being accessed from other countries. It would be useful if the guidance could provide guidance on the parties' obligations in this scenario.

76.2 Confidentiality agreements are commonly entered into in respect of such transactions. It would be helpful to have practical guidance on what is required in such agreements in respect of UK GDPR, e.g. processor clauses, agreements in respect of retention etc.

76.3 Often key employee data is disclosed in data rooms and other employee data is anonymised. Guidance on the legal basis for that difference and how to draw the distinction would be useful.

77. DISCIPLINE, GRIEVANCE AND DISMISSAL AND RETENTION OF RECORDS

77.1 Employees often ask for the meeting notes of interviews with other employees as part of grievances and disciplinaries. Guidance making it clear when these notes are and are not appropriate to share from a data protection perspective would be helpful. Guidance applicable to trade union representatives who may represent workers at these meetings (and may be joint data controllers under Article 26 UK GDPR) would be helpful.

77.2 Employees are not only using email, but also messaging and video systems like Teams, Slack, and Zoom at work. These are also used in respect of disciplinaries and grievances. It would be helpful to have guidance on the use of those platforms and the data protection requirements for using them generally – and in particular on how certain rights can/should be exercised in respect of those platforms where the data is often only retained for a very short period of time due to the company operating the platform.

78. OUTSOURCING DATA PROCESSING

78.1 Companies are becoming more internationally based, often headquartered in the US, and data needs to be shared within the group companies. This is a development which should be addressed in the guidance – including in respect of messaging and video systems like Teams, Slack, and Zoom at work.

78.2 Guidance on when consultants are considered to be "processors" of data rather than being able to process the data in the same way as an employee on behalf of the employer/controller would be helpful.

5C) MONITORING AT WORK

79. Aside from the arrival of the UK GDPR and the DPA 2018, case law changes and new guidance should be reflected in the new guidance.

ARTICLE 8 MONITORING CASES

80. Since the publication of the 2011 Code, there have been a number of important cases in the European and domestic courts regarding the compatibility of Article 8 of the European Convention on Human Rights (**ECHR**) and monitoring at work. These rulings remain relevant because the UK's membership of the ECHR is unaffected by Brexit.

81. Article 8 of the ECHR affords a right to respect for private and family life. Workers have a legitimate expectation that they can keep their personal lives private and are entitled to a degree of privacy in the work environment. Legitimate interests which can override Article 8 rights include health and safety, legal and regulatory obligations and the safeguarding of confidential information. As the 2011 Code makes clear, a balancing exercise needs to be carried out to judge whether the monitoring is a proportionate response, which will sometimes be by use of a DPIA.

82. However, there are further key principles and/or changes of emphasis deriving from this body of case law. A summary of these, and our suggestions for how these should be addressed in the new guidance, are:

83. In *Bărbulescu v Romania* (Application no. 61496/08) [2017] ECHR 742, the Grand Chamber of the European Court of Human Rights set out the following factors to consider when assessing Article 8 compliance:

    83.1 notice - whether clear advance notification of the extent and nature of the monitoring was provided;

    83.2 extent and intrusiveness;

    83.3 legitimate reasons;

    83.4 other means - whether there was a less intrusive method to achieve the same aim;

    83.5 consequences (for the employee); and

    83.6 safeguards - whether the employee had been provided with adequate safeguards.

84. This guidance is instructive for employers as to how such monitoring will be viewed by the courts. It would be helpful if the ICO could, to the extent possible, confirm if this guidance equates to its views (and if so, to consider whether it should set out its new guidance based on the same factors) or whether there are additional factors employers should consider when embarking on or making changes to their monitoring practices.

85. The *Bărbulescu* factors were also applied in the context of covert surveillance in the case of *López Ribalda and Others v Spain* [2019] ECHR 752. Again, the ICO might want to consider providing its guidance on the factors to be considered in deciding whether covert surveillance is proportionate in a similar format.

86. As a broader point, given the increased home and hybrid working as a result of cultural changes and COVID-19 (see further sections below), the new guidance could usefully confirm the extent to which the same factors are applicable to remote working (where expectations of privacy may be heightened) and/or whether there are additional considerations for employers.

87. The case law confirms that the extent to which an employee had a reasonable expectation of privacy in relation to the communications in question is crucial in determining infringements of Article 8. When identifying any likely adverse impact of the monitoring arrangement, employers should be encouraged to consider to what extent workers will have an expectation of privacy. This is different terminology than the language used in the 2011 Code at page 61 (which is confined to an employee's knowledge of the monitoring) and reflects the *Bărbulescu* case and *Atkinson v Community Gateway Association* [2015] ICR 1. The ECtHR has also confirmed that once an employee is told about allegations made against them, this removes any reasonable expectation of privacy in *Garamukanwa v United Kingdom* (Application 70573/17) [2019] ECHR 209.

88. The *Bărbulescu* case puts more emphasis on the content of the communication than the context in which it was made. For example, the fact the employer explicitly sought to reserve the platform for professional communications only did not mean that private communications on it lost their private status. It would be helpful if the ICO's guidance could extend to communications on systems that are not permitted to be used for private purposes, and also the boundaries of how far monitoring can extend to an employee's activity using a personal email account but which takes place on the employer's IT systems. We anticipate monitoring in these instances will only be justified rarely, if at all.

89. The new guidance should acknowledge the distinction between 'passive' monitoring (for example, monitoring the flow of communications to whether an employee is active on emails during work hours) and 'active monitoring' (for example, opening emails or similar facts to what was decided in *Bărbulescu*).

90. The content of an Electronic Communications Policy (page 69 of the 2011 Code) should include confirmation that relevant materials or communications found when monitoring electronic systems may be used as evidence in grievance, disciplinary or other investigations. For example, see *Garamukanwa* and *BC v Chief Constable of the Police Service of Scotland* [2020] CSIH 61.

91. In *BC*, it was found that WhatsApp messages exchanged between police offers could be used in disciplinary proceedings and a distinction was drawn between those who work in regulated industries (where expectations of privacy are lower) and those who do not. We think the new guidance should reference this distinction.

ARTICLE 29 DATA PROTECTION WORKING PARTY OPINION 2/2017 ON DATA PROCESSING AT WORK (THE ARTICLE 29 OPINION)

92. In 2017, the former advisory body to the EU for implementation of the GDPR by relevant Member States, the Article 29 Data Protection Working Party, issued an opinion on employee monitoring at work: https://ec.europa.eu/newsroom/article29/items/610169/en. This considered technological developments which have enabled more intrusive and pervasive ways of monitoring.

93. The Article 29 Opinion provides practical recommendations on nine common processing scenarios, for example, during the recruitment process, monitoring ICT usage at work and outside work, and time and attendance monitoring. Notwithstanding Brexit, the Opinion remains a useful source of guidance on the operation of the UK GDPR.

94. A number of interesting points are raised in the Opinion although sometimes more detail would be beneficial. Please see our response to Question 6(c) for our suggestions in this regard for the new guidance.

EDPB GUIDELINES

95. Following increased concern about ubiquity of video devices in modern life, the European Data Protection Board adopted guidelines on data processing in relation to the use of video devices in January 2020: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_en.pdf.

96. The guidelines are helpful, providing greater detail on issues like lawful basis and appropriate use. It gives practical advice, for example, using techniques such as masking or scrambling to fulfil SARs, recommending time periods for data storage and advising against using video surveillance recordings showing a demonstration in order to identify strikers. The ICO's guidance and the 2011 Code should be updated to reflect these issues.

TECHNOLOGICAL AND CULTURAL CHANGES

97. Rapid developments in advanced data analytics, artificial intelligence and data capture have given employers more sophisticated capabilities to access a substantially greater volume of information about their employees than 10 years ago. Technology is becoming more cost effective as there is greater competition amongst the technology providers. It is also less "visible" than traditional forms of monitoring like CCTV and has the potential to disproportionately intrude on employees' privacy.

98. The insights these tools can provide to employers about the productivity, engagement levels, and even happiness of their workforce, is of huge value to employers, particularly now when the way in which people work has moved significantly away from the traditional workplace-based model, to increased remote and hybrid working as a result of globalisation and the pandemic, blurring the distinction between work and home.

99. There is no doubt that some of these tools, if used to their fullest capability, are disproportionately invasive. However, technological advances have several important use-cases:

    99.1 Data security measures: Some tools are necessary for organisations to comply with other data privacy and legal obligations. For example, data loss prevention (DLP) software is generally considered an important technological security measure to protect personal and other data. Advancements in DLP software mean that when configured appropriately the technology can lead to more accurate and focused monitoring of activity across an organisation's systems, which enables organisations to adopt this important security feature in a way which meets data minimisation and proportionality principles;

    99.2 GPS and location tracking: These are common particularly in courier/delivery services to enable customers to have more accurate delivery times providing greater flexibility with customer's own

arrangements. Tachographs are also routinely used for logging hours of work for HGV drivers. These are essential to ensure compliance with statutory obligations under the Working Time Regulations 1998 and Road Transport (Working Time) Regulations 2005. However, these can also be disproportionately intrusive if they track employees' location during rest breaks or other private time;

99.3 Time recording and attendance systems: These tools are necessary to help meet legal requirements regarding tracking of working time and attendance records for fire and other emergency evacuations. They also help organisations like professional services firms meet other requirements such as accurate time recording for client and internal cross charging purposes, and profitability tracking / ensuring that future work is priced more accurately. However, advancement in this type of software can go too far, for example, when it uses employees' biometric data, or it is used for disproportionate further processing such as overly-intrusive monitoring of employee productivity;

99.4 Regulatory compliance: Employers are facing increased compliance obligations, particularly in regulated industries like the financial services industry where employers are required to take steps to prevent against market abuse, insider trading, bribery, corruption and anti-trust violations. But even more generally, for example, the government has announced that it will be legislating for a new positive duty on employers to prevent sexual and third party harassment in the workplace. In order to satisfy this obligation, there is an argument that employers have to be more proactive at troubleshooting potential breaches through employee monitoring rather than only reacting after a complaint. Again, left uncontrolled, this can be disproportionately intrusive. However, provided that the right balance is struck, it can be a very useful and important tool in helping to create a healthy, happy and diverse workplace culture;

99.5 Productivity and performance monitoring: This is the use-case that our members have seen generate the most controversy and suspicion from employees, particularly when managed through artificial intelligence and / or ADM. Advancements in this area can give managers the technical capabilities to have continuous and real time access to what applications their direct reports are using and for how long. But there are more benign technologies available, aimed at giving management aggregated insights that will enable them to make macro adaptions to the way they engage and manage their workforce, whilst providing individuals with insights which are personal to them and for their eyes only. The most difficult challenge arises from concerns about intrusions to the private life of individual staff, which can be particularly difficult where laptops and smart phones might be used for a blend of personal and work activities, such as managing social media accounts. In a world where work-life balance is becoming increasingly hard to attain, these productivity and engagement tools, if used with proper

controls and anonymisation where possible, can be beneficial to employer and employee alike; and

99.6 Health and wellbeing monitoring: These tools are necessary to help meet health and safety requirements in certain sectors such as manual and heavy industrial work. Outside of these very limited categories, employers will rarely have a lawful basis to regularly monitor their employees' health and wellbeing. There may be a basis to justify use of technology for continuous health monitoring in the context of an employer's ongoing obligation to make reasonable adjustments for disabled workers, although any use of technology in this way would need to be subject to the considerations for processing special category data. Despite potential limitations, the COVID-19 pandemic has caused us to explore new ways of working to get on with daily life, and there is an argument that wearable tech that tracks employees' health and distance from one another can be beneficial in helping those that cannot work from home or socially distance as a safer way of working. Such considerations must also take into account separate legal obligations in health and safety law.

100. We consider that it is important for the updated guidance to recognise that (increased) employee monitoring through new technologies isn't always unlawful, and in fact will often be lawful provided that appropriate compliance steps in place including:

100.1 establishing a genuine and lawful basis for the data processing;

100.2 examining whether the technology application is proportionate - normally through a 'legitimate interests assessment';

100.3 ensuring that data controllers have received relevant training to understand how the new technologies should operate;

100.4 being transparent with employees and their trade union(s) or representatives, and where appropriate, consulting with them before beginning to process data through the new technologies; and

100.5 completing a DPIA before beginning to process data through the new technologies and adopting any privacy risk mitigation measures, such as producing an APD and complying with the additional safeguards for processing special category data.

101. We thought it might be helpful to identify various monitoring technologies, which we have grouped into types / use-cases:

101.1 Video / physical surveillance – The likes of CCTV have been in existence for some time. They are primarily used for security purposes rather than monitoring employees' activities but some employers do use video

surveillance to track employee location, real-time activities and productivity, and as evidence in the case of suspected wrongdoing (for instance, allegations of theft in retail). New functionalities include facial recognition software and sound recording;

101.2 Employee monitoring hardware - Hardware monitoring includes tools such as wearable tags, pressure sensors for chairs and desk occupancy detection sensors;

101.3 Web, app activity and email monitoring – These systems are generally used to ensure the safety and proper use of company computers and mobile devices;

101.4 Call recording / phone tapping – These are typically used for quality and training purposes, but are sometimes used as evidence in the case of suspected wrongdoing (for instance, allegations of abuse against a customer);

101.5 Health and wellness monitoring – These can range from wearable tech that measures heart rate, blood pressure and stress levels to “sentiment analysis” tools that can measure an employee’s level of happiness, engagement and morale;

101.6 Time and attendance software – Software apps to record attendance and billable hours are not new. However, functions now include applications that can log keystrokes and mouse movements, capture screenshots, monitor applications usage, enable webcams and collect footage. These can also be put onto mobile devices, which can give rise to additional complexities if the employee uses their own device for work purposes;

101.7 Social media monitoring – both in the context for recruitment purposes and during investigations;

101.8 GPS and location tracking, and event data recorders – particularly common for mobile employees; and

101.9 Mobile device management – these enable employers to locate devices remotely, deploy specific configurations and/or applications, and delete data on demand.

THE IMPACT OF COVID-19

102. There were significant employment law concerns that arose in response to COVID-19 and the lockdowns introduced.

103. In the context of monitoring at work, this was most obviously seen in the following areas:

103.1 More people working from home;

103.2 Furlough and flexible furlough under the Coronavirus Job Retention Scheme;

103.3 Health matters arising from sickness related to COVID-19;

103.4 Management of risks from changes and / or return to a workplace location.

104. A further issue arose from a change in priorities for enforcement by the ICO in matters arising from when the pandemic began.

MORE PEOPLE WORKING FROM HOME

105. On 16 March 2020, the Prime Minister announced that people should work from home where possible. While there were different positions that applied by the devolved administrations, as well as debate on whether the instruction was a matter of guidance or law at different times in different places, this situation continued until August 2021.

106. Consequentially, there was a cultural change in many people working from home and this accelerated the development of data-driven technologies in certain industrial sectors which sparked debate on how these systems might be used fairly to balance the commercial interests of employers against the individual rights (such as to respect for privacy) of staff affected. It also highlighted challenges for employers to comply with health and safety law.

107. More detail of how these technologies have operated to monitor staff are explained above. However, it is widely reported that many employers expect a high proportion of their staff to continue working from home into the future, so we can expect the debate on how these technologies operate to continue. Therefore, more detailed guidance on how data protection law and employment law interface for those working at home would be welcome. In particular, the extent to which (and when) DPIAs should be used when using 'new technologies' to monitor staff.

FURLOUGH AND FLEXIBLE FURLOUGH UNDER THE CORONAVIRUS JOB RETENTION SCHEME

108. The Coronavirus Job Retention Scheme (**CJRS**) introduced the concepts of furlough and flexible furlough, enabling many employers to receive funding from HMRC in order to pay the wages of PAYE staff. The CJRS began in March 2020 as a response to the impact of lockdowns on business and lasted to 30 September 2021. It is estimated by the ONS that a quarter of people who have been employees during the pandemic were furloughed at some point since March 2020.

109. A fundamental feature of the scheme was that staff must not work for the employer, or an associated employer, while furloughed. Flexible furlough commenced in July

2020 and enabled an employer to negotiate part-time working with their staff while continuing to receive payments under the CJRS to top up the proportion of wages when the individual was not required to work.

110. In March 2021, the UK Government announced the creation of a taskforce to help HMRC investigate fraud of approximately £4 billion accessed under the CJRS. Examples of fraudulent claims under the CJRS include:

110.1 Claims under the CJRS for non-existent PAYE staff;

110.2 Claims for PAYE staff who continued to work normally for the employer, or for an associated employer; and

110.3 Misrepresented hours of work by PAYE staff.

111. Typically, employers need to show data that explain whether staff were working at the times it was claimed they were furloughed in the application made to the CJRS. While this type of data might include timesheets and other traditional monitoring techniques, it may also include data processed by (or on behalf of) the HMRC and its investigators.

112. It seems likely that investigations (and processing the data that underpin decisions made) will continue for some time yet, particularly if the topic falls within scope of any Inquiry into COVID. Therefore, the ICO may wish to consider how guidance can be given for third parties who process data monitoring staff at work.

HEALTH MATTERS

113. Up to 1 October 2021, it is estimated there have been 7,850,000 cases of COVID-19 in the UK. While it is difficult to know precisely, a significant proportion of these cases would have been individuals employed by a business.

114. Workers who suffered sickness after contracting COVID-19 would normally be entitled to receive sick pay. Prior to the pandemic, the UK's relatively complex legal basis for statutory sick pay ('SSP') defined when an individual worker was entitled to receive a capped weekly payment for up to 28 weeks when absent from work due to incapacity and other qualifying conditions. For some workers, SSP will be enhanced by a contractual sickness benefit by an employer.

115. In response to concerns about the availability of SSP, particularly that the qualification criteria were too narrow, legislation was introduced in March 2020 to temporarily widen the circumstances in which it may be paid in relation to COVID-19 related absences.

116. It is axiomatic that a worker must inform their employer about the sickness in order to qualify for (and receive) sick pay. Health data is a special category data under

UK GDPR and DPA 2018. This means the data controller for an employer must use an APD and adequate safeguards in order to process this type of data.

117. A further issue arises in the monitoring of vaccination status and how the processing of this data is affected. ELA has responded separately to the UK Government's consultations on this.

118. As the monitoring of an individual's health matters relating to COVID-19 is an ongoing obligation during the pandemic, and most employers would be using new technologies to do so, it is likely to require the employer to have conducted a DPIA. This is because Article 35(1) UK GDPR requires data controllers to do this where processing results in a high risk to the rights and freedoms of natural persons.

119. This sub-topic is another area where data protection law, employment law and health and safety law overlap. For example, any future guidance might wish to consider that employers are also obliged to monitor and report cases of COVID-19 infection where exposure occurs as a result of a person's work under the Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 2013 ('RIDDOR'). Additionally, as with other measures introduced in relation to health and safety law, the employer must consider its obligations to inform and consult with the recognised trade union (or elected representatives) of staff affected.

MANAGEMENT OF RISKS FROM CHANGES AND / OR RETURN TO A WORKPLACE LOCATION

120. We have commented elsewhere in this response about considerations to monitoring of staff who are working from home. The monitoring of staff who change or return to a workplace location overlaps to an extent with those points, especially where individuals work partially at home and partially in another workplace location.

121. While COVID-19 continues to play such an important part in all our lives, a common scenario will see an employer needing to assess and update assessments of risks for the monitoring of an individual at the same time in both data protection and health and safety law where there is a change and / or return to a workplace location.

5D) INFORMATION ABOUT WORKERS' HEALTH

COVID-19 AND WORKPLACE HEALTH ASSESSMENTS

122. The ICO has already provided substantial guidance relevant to employers on how they should lawfully process the health data of their workers during the Covid-19 pandemic through its data protection and coronavirus information hub. As mentioned above in Question 4, given the changing nature of the pandemic and the importance of up-to-date guidance on this issue, we recommend that the employment practices guidance does not go into detail on Covid-19 specific issues, but that the ICO continues to update its Covid-19 specific guidance separately. The

employment practices guidance should, however, cross-refer to the Covid-19-specific guidance where appropriate.

123. As mentioned above, the Covid-19 pandemic has led to greater changes in working conditions and employers' practices on the collection of health data. Further changes to working patterns are anticipated, such as potential legislative changes to the right to request flexible working. As a result of these changes, employers are more aware of their duties to carry out health and safety risk assessments and the information that they need to collect in order protect their workforce and the general public.

124. One challenge employers face is that the move to increased remote/hybrid working makes it more difficult to spot signs of mental ill-health (e.g., punctuality, appearance, interpersonal behaviour in the office). As a result, employers may feel the need to monitor employee health more proactively, in order to ensure that health conditions are appropriately accommodated. They may also need to collect further data regarding physical conditions so that they can provide appropriate homeworking equipment and provide a safe place to work. Guidance on collecting this data with a minimum level of intrusion would be helpful – as would guidance on how employers could manage the overlap in their obligations to inform and consult employee representatives under both health and safety and data protection legislation.

HEALTH-TRACKING TECHNOLOGIES AND EMPLOYEE WELLNESS PROGRAMS

125. Since the publication of the 2011 Code, there has been a substantial uptake in employers seeking to implement employee wellness programs.

126. Employers may wish to assess which schemes employees would like to participate in and survey how employees engage with employee benefits such as cycle to work schemes, private medical insurance, discounted or free wearable technologies or specific competitions and challenges that involve an employee sharing their health data (e.g., access to health data on an employee-owned wearable device). We suggest that the employment practices guidance addresses gathering this information in a lawful and appropriate manner, and highlights the importance of appropriate communications with employees (compliant with the extensive duties under Articles 12-14 UK GDPR) about what data is being gathered and for what purpose, not least because there may be concern amongst employees that employers are using these schemes as a means of monitoring their health more generally.

BIOMETRIC VERIFICATION

127. The development of facial and fingerprint recognition technologies have led to some employers considering introducing such technologies within the workplace (e.g., for health and safety purposes to identify members of staff). Given the potential risks

inherent in the use of these technologies, and the need for a DPIA and consultation under Article 35 UK GDPR, it would be useful for employers to have more guidance in this area.

QUESTION 6

WHAT ISSUES ABOUT THE FOLLOWING TOPIC AREAS WOULD YOU LIKE TO SEE GUIDANCE ON?

6A) RECRUITMENT, SELECTION AND VERIFICATION

128. In our view, employers would benefit from practical and workable guidance on the following issues in particular:

UNSTRUCTURED DATA

128.1 One of the challenges of processing unstructured data is that it cannot reasonably be said that all of the personal data contained within emails (to take one example) is necessary for the employer or prospective employer or recruitment consultant to process. Some of this data will inevitably arise or be collected in passing, especially given the rise in home working and the blurring of lines between work and home. This is particularly important where unstructured data contains the special category data of the job applicant or employee, or even of their families (for example, where this appears in the background of a Teams meeting or interview).

128.2 Those involved in the recruitment process would benefit from guidance as to how to handle personal data, including special category data, which is collected in an unstructured way that is outside of the data controller's control. With respect to special category data, there is a need for guidance on the lawful condition for processing where there is no obligation to do so under applicable employment law. It may be that guidance should recognise that consent should be expressly acknowledged as acceptable in the context of certain processing in the employment relationship, including criminal records checks (see above),processing of unstructured special category data and automatic decision- making (see below). Alternatively, it may be necessary to provide guidance that makes clear there should be a deliberately wide interpretation on the meaning of Article 9(2)(b) UK GDPR and the corresponding provision in UK law to allow employers, prospective employers and recruitment consultants to carry out the processing which is necessarily carried out in the context of an employment or recruitment relationship.

128.3 Responding to SARs in a recruitment or promotion setting, in particular as it relates to unstructured data, can be difficult to manage and employers may consider it is becoming disproportionate. Notwithstanding the clear benefit which individuals derive from the right to make a SAR in this context (and

the importance of being able to obtain information as to an employee's treatment and their data generally), it is not uncommon for employers or prospective employers to expend extensive resources when responding to SARs. This is an opportunity for the ICO to consider whether a data subject's right to access might be revisited in terms of addressing inaccuracies in structured data or other data on which recruitment decisions may be made (for example, data used for profiling).

128.4 Unstructured data also presents immeasurable issues for employers, prospective employers and recruitment consultants who are seeking to comply with their obligation to ensure data minimisation:

(A) We would welcome guidance, in any event, on the technological challenges of deletion given that the ICO has since removed its previous guidance on the meaning of "delete", "irretrievably delete" and "put beyond use".

(B) In addition, there is a real need for pragmatic guidance on dealing with the practical issues related to unstructured data and deletion, given that no organisation can afford to employ people or engage technologies to wade through unstructured data for the personal data of particular individuals. In our experience, employers' data deletion / retention policies are typically not equipped to deal with this issue. Not only does this mean that it is difficult to delete unstructured personal data (particularly contained in back up tapes) but it also means that thinning of personal data contained in unstructured sources such as email accounts is a practical impossibility.

DIVERSITY AND WORKPLACE AUTHENTICITY

128.5 In general, it is important that future employment practices guidance is drafted to co-exist or complement pre-existing or future requirements from other regulators (such as the FCA, PRA and Bank of England).

128.6 In respect of diversity data, guidance should include:

(A) The extent to which employers or prospective employers can make the collection of diversity data mandatory rather than voluntary;

(B) The purpose for which employers or prospective employers can appropriately use special category personal data and the lawful basis for processing and retaining such data, given it is unlikely to be necessary for an employment obligation or right; and

(C) How employers or prospective employers should treat special category personal data where such data would otherwise be aggregated but the sample sizes are too small to genuinely anonymise the data.

128.7 With respect to the lawful basis for processing and retaining such data, if consent is the appropriate Article 9 UK GDPR condition, guidance should include further details as to how this is appropriate in the employment relationship.

128.8 In respect of workplace authenticity, we would be grateful for guidance on how employers and prospective employers can avoid mishandling or inappropriate use of unstructured special category personal data voluntarily shared by employees and job applicants.

ROLE OF THIRD-PARTIES IN THE RECRUITMENT PROCESS

128.9 Particularly where employers use third-parties in their recruitment processes (such as recruitment businesses or professional screening providers), we would be grateful for guidance on the circumstances – if there are any – in which:

(A) an employer can comply with its notification obligations by delegating the act of notifying a candidate of its privacy policy to the third party (i.e. is it sufficient for a recruitment business to notify a candidate of an employer's privacy policy, or must there be a direct notification from the employer to the candidate?);

(B) a recruitment or employment agency can rely upon the legitimate interests of or employment obligations of the prospective employer.

128.10 We request that any future guidance details the ICO's expectations regarding how personal data should be handled and processed in such circumstances, including in particular how and when it is permissible for such data to be used to inform decisions to (i) approach a potential candidate and (ii) assess that candidate in the application stage.

128.11 It would also be of assistance for the guidance to address the appropriate retention periods for such data, in particular when it is appropriate to retain that data in respect of unsuccessful candidates. Guidance on "standard" periods of retention for employers would be helpful.

(A) In the current economic climate, it is of benefit to both those recruiting and potential applicants for data to be retained for longer than the limitation period for employment tribunal claims (as was suggested in the 2011 Code).

(B) Indeed, as part of some diversity and inclusion monitoring processes it is important to retain personal data of unsuccessful candidates in order to track their success at other organisations in the immediate future.

(C) We have seen significantly delayed claims in the #metoo environment. Claims that are potentially legally out of time might still warrant or require internal investigation in the public interest generally or for regulatory reasons.

(D) Finally, contract claims can be for brought for up to 6 years in some circumstances.

128.12 In the recruitment context, it would be helpful to have guidance on the status of recruitment businesses (i.e. whether they are processors or controllers). The 2011 Code suggested that the relationship was one of controller to controller and it would be good for this to be restated.

128.13 As stated in answer to Question 4, in the context of verification, we would be grateful for guidance to resolve the conflict between the conditions in the UK GDPR and requirements of any applicable statutory or regulatory pre-employment screening processes (such as, for example DBS checks and, in the financial services context, fit and proper person reference requirements), as well as additional guidance on the circumstances in which it is legitimate for employers to know whether applicants have a criminal record.

REMOTE RECRUITMENT

128.14 We would be grateful if future guidance were to address the ICO's expectations regarding how personal data contained in video interviews (or any other data processed in meetings held remotely) is processed, stored, shared and retained and, in particular, the exercise of rights by a data subject. For example, it would be useful to know what the ICO considers to be a "reasonable and proportionate search" in the context of files where the context cannot be so easily searched, such as video files, instant messaging or messaging apps and texts on work devices.

128.15 The guidance should also address the interplay with previously published ICO guidance on the inference of special category personal data from names and images and clarify the extent to which video interviews result in the collection of special category personal data. It would be unfortunate if recruitment agencies or prospective employers inadvertently collected such data in circumstances in which there was no employment obligation to do so and in which consent was inappropriate because of the imbalance of power between prospective employers and job applicants.

COVID-19 AND VACCINATION

128.16 As above, it is foreseeable that more employers (particularly in healthcare settings) will seek information in respect of an applicant's COVID-19 vaccination status (as well as whether they have a negative COVID-19 test or immunity) as part of their recruitment decisions. Previous guidance published by the ICO indicated that employers could seek COVID-19 information, including vaccination data, where the employer had legitimate interests and subject to other data protection obligations, such as the need to carry out a DPIA.

128.17 It would be helpful for confirmation that such guidance applies also to prospective employers and employment or recruitment agencies processing the health related data of job applicants in order to place candidates. We would like to strengthen the guidance around the meaning of Article 9(2)(b) UK GDPR so that it is clear it extends to recruitment consultants as if they were employers (particularly given recruitment consultants are often subject to the same employment obligations, such as equalities law).

128.18 It would also be helpful to have further detail as to the kind of legitimate interests that would be sufficient to outweigh the risk to rights and freedoms of the data subject in the context of a high risk event such as denial of job opportunities.

ADM/USE OF AI IN RECRUITMENT

128.19 As noted above, given the increasing use of ADM in the recruitment process, guidance on how a potential employer can use such AI and what the candidate must be told about that process and their rights would be helpful.

128.20 The existing guidance is not fit for purpose and does not accurately or clearly delineate between decisions made solely by automatic means without human intervention and automated processes that assist human decision-making. Most importantly, a number of the examples contained in the existing guidance do not amount to ADM within the definition of Article 22 UK GDPR. This has led to a lack of clarity for employers, prospective employers and recruitment consultants.

128.21 In particular, it would be helpful if the guidance could include (i) the definition of a decision, (ii) the extent to which human intervention at the input phase is sufficient to take an automated process outside of the scope of Article 22 UK GDPR and (iii) the degree of human intervention or review required before or at the output phase.

128.22 It would also be helpful for guidance to focus on the extent to which ADM applies to (a) filtering, (b) ranking or (c) shortlisting of job applicants by a

computer applying criteria set by a human – while there may be a tendency for organisations to make default declarations that they are not using ADM processes even where this may not be correct, it would also be regrettable if organisations who were not making decisions with legal or other significant effect by solely automated means were mistaken as to the remit of Article 22 UK GDPR. We do not believe that the current guidance appropriately engages with this and it is potentially misleading as to what is and isn't ADM.

128.23 The guidance could also helpfully focus on the level of scrutiny and/or testing required in order to defend against challenges of bias in the recruitment process.

INTERNATIONAL RECRUITMENT

128.24 Given the international aspect of recruitment for many employers, it would be helpful if the guidance could address what steps potential employers can and should take where there is an international element to the recruitment process (either the employer or the employee is based outside the UK, which necessitates the transfer of personal data across borders).

128.25 In particular, it would be helpful for the guidance to provide clarity and examples on the use of derogations to enable international transfers (including third-party transfers of data) in the recruitment process and, in particular, the transfer of data between (i) employer and recruiter and (ii) employer and outsourced employee screening providers.

6B) EMPLOYMENT RECORDS

129. In our view, employers would benefit from practical and workable guidance on the following issues in particular:

130. PENSION AND INSURANCE RECORDS: It would be helpful for this section to cover third parties that process employee personal data more generally, such as payroll, benefits providers and occupational health (including where international transfers are involved).

131. **EQUAL OPPORTUNITIES MONITORING**

131.1 We consider that it would be helpful if the ICO gave some practical guidance on appropriate questions to ask. In particular, we consider that including a "prefer not to say" option would be good practice.

131.2 The current guidance states that data collected for equality and diversity monitoring should not be used for any other purpose. It is increasingly common for businesses to be required to share/published anonymised diversity statistics, for example when participating in external pitches or third

parties. It would be helpful if the ICO acknowledged this and provided some guidance on what legal basis can be relied upon in this situation.

132. **MARKETING**: We consider that this guidance should direct employers to the ICO's marketing guidance.

133. WORKERS' ACCESS TO INFORMATION ABOUT THEMSELVES

133.1 SARs are increasingly common and a difficult area for employers to navigate themselves due to the number of considerations including compiling the data, redacting data for any third party data where appropriate and securely providing the results to the subject. We consider it would be beneficial for employers to be given concise but detailed guidance on how to deal with SARs, and to alert employers to when they can refuse or query a SAR, and what resultant impact this has on their timescale for responding to a SAR.

133.2 Equally, employees would benefit from more guidance on how they can use SARs in an employment context, for example, as to the breadth and reasonableness of a SAR, and how to consider the range of documents that are required. Both sides would benefit from guidance as to use of the SAR procedure, so as to meet the employee's aims, without unduly (and unnecessarily) exhausting the employer's resources.

133.3 We note that the ICO has previously worked on a consultation specifically in relation to publishing guidance on the right of access, in which it was identified that employers lacked certainty on their ability to refuse to comply with a SAR, and on when they can "stop the clock" for responding to a SAR to seek clarification. We consider it would be helpful for the published guidance on the right of access to be referenced within this guidance, and further information on the "stop the clock" issue provided.

134. **REFERENCES**: Guidance would be useful on when the exemption relating to confidential references could apply.

135. **DISCLOSURE REQUESTS**: It may be helpful to refer to other sources of ICO guidance, given there are a number of factors to consider when deciding whether or not to disclose to external parties.

136. **OUTSOURCING DATA PROCESSING** AND **RETENTION OF RECORDS:** It would be helpful to deal with the practicalities of global companies and the transfer of employee data. These sections should also reference other ICO guidance on this topic and should be cross-examined to ensure they are consistent and does not conflict.

6C) MONITORING AT WORK

137. The Article 29 Opinion expressly says that the employer "is very unlikely to have a legal ground under legitimate interest, e.g. for recording an employee's keystrokes and mouse movements". It also advises employers against using facial recognition technologies.

138. It would be helpful, to the extent possible, for the ICO to advise what types of employee monitoring they consider are typically likely or unlikely to satisfy a legitimate interest. Similarly, it would be helpful to have examples of the types of monitoring that are sufficiently high risk, in the ICO's view, to require a DPIA to be carried out. For example, the Opinion states that a DPIA should be performed prior to the deployment of any mobile device management technologies that are new, or new to the data controller.

139. Other areas where we would like to see guidance are:

139.1 Bring your own device policies – the 2011 Code focuses on ensuring personal data processed by employees on their own device on the company's behalf is appropriately protected. The broader question is the extent to which the employees' own personal data is impacted - for instance in the event of suspected wrongdoing and the employer demands the device is provided for examination.

139.2 Investigations and particularly when (or if) it may be lawful to monitor an employee's activities / communications outside work e.g., personal emails, instant messaging services, social media such as WhatsApp, Facebook, Twitter, LinkedIn etc. A sub-section on investigations would be well-received, in particular confirmation that the same general monitoring considerations apply but that the thresholds are different.

139.3 Lawful basis for monitoring where monitoring may 'inadvertently' access special category data. For instance, an investigation into suspected theft of confidential information, where the employer searches email records and reviews them. Are Article 9 UK GDPR ground(s) always necessary where the access is inadvertent and the special category data is immediately deleted? If Article 9 UK GDPR ground(s) are required, to what extent can Schedule 1 Part 2 DPA 2018 grounds (in particular paras 10, 12 and 14) be relied upon by employers?

139.4 The extent to which Article 35(9) UK GDPR requires consultation between an employer and its staff and their representatives (including trade unions) before processing of data with new technologies commences.

6D) INFORMATION ABOUT WORKERS' HEALTH

COVID-19 AND WORKPLACE HEALTH ASSESSMENTS

140. As briefly mentioned in the ICO's guidance on special category data, employers will often need to rely on the condition in Schedule 1, condition 1 of the DPA 2018 in order to justify the processing of health data when ensuring the health, safety and welfare of employees.

141. The text of Schedule 1, condition 1 of the DPA 2018 states that the processing of special category data (including health data) is permitted for the purposes of performing obligations or rights conferred by law on the employer "*in connection with employment, social security and social protection".* It would be useful if the ICO could clarify the scope of legal obligations that may justify processing under this condition further, particularly in the context of employers needing to seek more information on employee health than may have been the case in the past (see our response to Question 5(d) above).

142. Currently the ICO's guidance on special category data states that employers should be able to "identify the legal obligation or right in question, either by reference to the specific legal provision or else by pointing to an appropriate source of advice or guidance that sets it out clearly". Employers will benefit from further information on which sets of guidance they can reference to justify processing activities (for example, Acas guidance or guidance issued by the Health and Safety Executive). To assist employers with planning processing activities involving health data, the ICO should provide more guidance and case studies that elaborate on the threshold of "necessity" under this condition. Additional information on whether employers may also rely on the substantial public interest condition in Schedule 1 of the DPA 2018 for "protecting the public" as another condition for processing health data to safeguard employees would be similarly helpful.

HEALTH-TRACKING TECHNOLOGIES AND EMPLOYEE WELLNESS PROGRAMS

143. As employee wellness schemes become more commonplace in the workplace and wearable technologies become more pervasive, employers will benefit from guidance on how they should lawfully introduce and implement such schemes and technologies.

144. In particular, employers will benefit from clear guidance on how and when they may rely on explicit consent as a condition under Article 9 UK GDPR for the processing of employee health data for such voluntary schemes and the steps that employers should take to demonstrate compliance with UK GDPR.

BIOMETRIC VERIFICATION

145. We note that the ICO is planning to produce more detailed guidance on processing biometric data (see here). It may be helpful for the revised guidance to also consider how employers may lawfully introduce identification technologies such as facial recognition within the workplace and the lawful bases and conditions that

employers may rely on to do so under UK GDPR (please see our response to Question 4 for additional information on lawful bases and conditions).

QUESTION 7

ARE THERE ANY CASE STUDIES OR SCENARIOS THAT YOU WOULD LIKE TO SEE INCLUDED IN THE EMPLOYMENT PRACTICES GUIDANCE?

7A) RECRUITMENT, SELECTION AND VERIFICATION

146. We consider that employers would be assisted by case studies on the following issues:

146.1 The processing of health-related data in the recruitment context, particularly data in respect of an individual's COVID-19 vaccination status;

146.2 The circumstances in which an employer is permitted to retain information in respect of unsuccessful candidates, the legal basis(es) for doing so (including confirmation if consent is inappropriate), for how long such data may be retained and the purposes for which it may be used;

146.3 The circumstances in which personal data may be shared with external bodies in the context of measuring diversity and the type of personal data that may be shared. While issues will not arise in respect of statistics that are aggregated and genuinely anonymised, small data sets are very common and it may not be appropriate or even possible to sufficiently anonymise or aggregate the data. Such guidance should focus in particular on organisations to which an employer may be required to report (such as a regulator) on the one hand, and organisations to which it may be desirable to report (such as to awarding bodies such as Athena Swan or clients in a pitch context or as part of regular reporting for a client of the diversity of their client teams) but where such reporting falls short of a legal obligation;

146.4 The collation and processing of personal data when conducting pre-employment screening for those employers (such as Early Years providers or those in regulated sectors) who are subject to Safer Recruitment or regulatory requirements;

146.5 The collation and processing of personal data in the context of "head-hunting", including when in the process individuals must be made aware of a privacy policy. By way of example, a recruitment business may collate information from third party sources (such as social media, particularly LinkedIn, or Google searches) and use that information to decide internally whether to approach the data subject in respect of an employment opportunity. To comply strictly with UK GDPR, the recruitment business ought to send its privacy notice to the data subject prior to processing their personal data (i.e. prior to discussing internally whether to approach the

data subject regarding the opportunity), however this does not accord with practical reality, whereby a data subject would not be approached until a decision to do so had been made. It is also not an answer to say that the privacy policy can be directed to individuals before the processing can take place as it is often necessary to process data in order to make an assessment as to whether an introduction is necessary or appropriate;

146.6 Examples of international recruitment and the cross-border transfer of data;

146.7 Examples of ADM and what is permissible.

7B) EMPLOYMENT RECORDS

147. **PENSION AND INSURANCE RECORDS**: In light of the Article 28 UK GDPR requirements, it would be helpful if the guidance included guidance on what it considers to be a controller-controller or controller-processor relationship and how and employer can make that determination.

148. **EQUAL OPPORTUNITIES MONITORING**: We consider that it would be helpful if the ICO provided guidance to employers on the questions to be asked as well as some case studies to caution employers on when publishing survey results will inadvertently reveal an individual's identity and special category data.

149. **WORKERS' ACCESS TO INFORMATION ABOUT THEMSELVES**:

149.1 Given the points raised above in relation to the need for greater guidance on SARs, we consider it would be of great benefit for employers to read a case study of an employer dealing with a request from start to finish. Whilst larger companies may have established systems for dealing with SARs, the guidance would assist small to medium sized companies with this process.

149.2 A worked example could include the employer seeking clarification as to the nature and scope of the request, or an example of a request that could potentially be considered manifestly unfounded or excessive by an employer.

150. **REFERENCES**: A worked example demonstrating an employer's ability to refuse to disclose a confidential reference where the exemption would apply.

151. **PUBLICATION AND OTHER DISCLOSURES**: A case study on publishing marketing information on an employer's social media could be of benefit, for example a photo of a team-building away day.

152. **MERGER, ACQUISITION AND BUSINESS RE-ORGANISATION**: A worked example of the global complications caused by data room hosting and the international nature of companies would be useful.

153. **DISCIPLINE, GRIEVANCE AND DISMISSAL**:

153.1 A case study on when an employee wants the meeting notes or details in respect of other employees in a disciplinary or grievance process would be helpful.

153.2 It could also be useful for the ICO to refer to *Kathryn Hopkins v The Commissioner for HMRC* [2020] EWHC 2355 (QB) and to provide commentary on the same, given the interesting overlap between disciplinaries in the workplace, the sharing of data internally and the relevance of external investigations.

154. **OUTSOURCING DATA PROCESSING**: A case study which shows the practicalities of global companies and the transfer of employee data and what steps to take would be useful.

155. **RETENTION OF RECORDS**: It would be useful for the ICO to provide guidance/examples of appropriate/suggested retention times based on the requirements for employers to keep various different types of data as required by non-data protection laws (i.e. in relation to health and safety, for tax purposes, for the defence of legal claims etc).

7C) MONITORING AT WORK

156. It would be useful to see a case study on the use of CCTV, particularly through an employment rather than a commercial/customer lens, taking into account newer functions like facial recognition and integrated sound recording.

157. In the context of monitoring at work, we would like a worked scenario on how Article 22 UK GDPR is likely to be engaged by technologies that use AI and / or ADM. In particular, this would be most helpful if it addressed the processing of special categories of data to show how the APD and additional safeguards might be used.

7D) INFORMATION ABOUT WORKERS' HEALTH

COVID-19 AND WORKPLACE HEALTH ASSESSMENTS

158. Further case studies that provide examples of employers carrying out processing to justify the health and safety of their employees will be useful. For example, the ICO should build upon the "good practice recommendations" section in Part 4 of the 2011 Code to develop more specific examples of employers processing health data for health and safety purposes (e.g., case studies of drug and alcohol testing in the workplace and health screenings).

HEALTH-TRACKING TECHNOLOGIES AND EMPLOYEE WELLNESS PROGRAMS

159. Similarly, employers will also benefit from specific examples on the circumstances in which employers may rely on explicit consent as a condition under Article 9 UK GDPR to process the health data of their employees, despite the imbalance of power between the employer and the employee that would usually mean that explicit consent cannot be obtained. In this regard, employers would likely welcome guidance as to how requests for consent should be worded so as not to be seen to place undue pressure on the employee.

160. Additional case studies and scenarios that may be helpful in this context include: competitions whereby employees share their fitness activities with their employer; voluntary surveys on health and wellbeing carried out by employers; and an employer providing wearable technologies (such as a smart-watch) to employees which allow employees to share their fitness activities with other employees.

QUESTION 8

DO YOU HAVE ANY OTHER SUGGESTIONS FOR FUTURE EMPLOYMENT PRACTICES GUIDANCE?

161. In order to make the employment practices guidance more accessible, we recommend that the ICO considers consolidating its input from the 2011 Code, the supplementary guidance and the quick guide into a single, accessible guidance document, accessible via the ICO's website and via PDF. As the supplementary guidance to 2011 Code and the quick guide do not form part of the 2011 Code itself, the status of each document is unclear and this creates uncertainty for employers seeking to implement policies based on the ICO's guidance.

162. However, we note that for workers and SMEs, a shorter, more accessible version of the guidance may still be useful. Therefore, we also propose that the ICO also considers publishing a shorter version of the guidance (either as part of the ICO's SME hub or within the ICO's Guide to the GDPR), which references and provides links to the more detailed guidance.

163. We also suggest that the ICO reconsider the current structure of the 2011 Code, in particular the use of numbered Good Practice Recommendations followed by unnumbered 'Key points and possible actions'. It is unclear what distinction there is between these sections, and there is a fair amount of repetition in the content.

164. On a similar theme, we suggest that the new guidance should distinguish more clearly between what the law requires, and what the ICO considers to be good practice.

165. Finally, it would be useful if future updates to the guidance were not only publicised (so that users would know when and how the guidance had been updated), but previous versions retained for historic reference. Ideally, the content of updates would be flagged so that users can easily see what has changed.

QUESTION 9

ABOUT YOU

We are answering these questions as a representative of a professional/industry/trade association or body.

QUESTION 10

PLEASE PROVIDE THE NAME OF THE ORGANISATION THAT YOU ARE REPRESENTING.

The Employment Lawyers Association.

QUESTION 11

HOW WOULD YOU DESCRIBE YOUR ORGANISATION?

See the Introduction on page 1 of this response.

QUESTION 12

WE MAY WANT TO CONTACT YOU ABOUT OUR EMPLOYMENT PRACTICES GUIDANCE AND SOME OF THE POINTS YOU HAVE RAISED. IF YOU ARE HAPPY FOR US TO DO THIS PLEASE PROVIDE YOUR EMAIL ADDRESS:

LandPChair@elaweb.org.uk

EMPLOYMENT
LAWYERS
ASSOCIATION

Members of this Working Group:

Anna Dannreuther	Field Court Chambers	Co-Chair
Clare Fletcher	Slaughter and May	Co-Chair
Ann Bevitt	Cooley (UK) LLP	
Elizabeth Bradley	Clarkslegal LLP	
Nicola Geary	DAC Beachcroft LLP	
Annabel Gillham	Morrison & Foerster (UK)	
Noella Gooden	Family Action	
Michael Hibberd	Doyle Clayton	
Deborah Margolis	GQ|Littler	
Jessie Mark	Curzon Green	
Sian McKinley	Herbert Smith Freehills LLP	
Lisa Rix	GQ|Littler	
Bruce Robin	UNISON Legal Services	
Jessica Shemmings	Rackspace	
Lucy Sorell	Deloitte LLP	
Matthew Warren	Wards Solicitors	
Julia Wilson	Baker & McKenzie	
Dan Alam	Morrison & Foerster (UK)	