Privacy International's response to the ICO consultation on draft employment practices – recruitment and selection guidance

February 2024

About Privacy International

1. Privacy International (PI) is an international non-governmental organisation that campaigns against companies and governments that exploit individuals' data. PI employs specialists in their fields, including technologists and lawyers, to understand the impact of existing and emerging technology upon data exploitation and our right to privacy.

2. Given our leading and respected status as a voice on issues of data and privacy, we are frequently called upon to give expert evidence to parliamentary and government committees. Among others, we have advised and reported to the Council of Europe, the European Parliament, the Organisation for Economic Co-operation and Development and the UN Office of the High Commissioner for Human Rights.

3. PI has a longstanding relationship with the ICO and has previously responded to a variety of consultations issued by the ICO as well as complaints related to data protection and information rights.

Introduction

4. PI welcomes the publication of the ICO's draft guidance on recruitment and selection (the "Guidance"). As the Guidance acknowledges, recruitment procedures frequently involve the deployment of novel technologies through which "*organisations are processing increasingly large amounts of information about people*".[1] The increase in the volume of data collected and the use of new AI based algorithms pose challenges for the privacy and data protection rights of candidates going through the recruitment process.[2] In particular, there is a risk of discriminatory and biased recruitment decisions, of negative impacts on worker

[1] See ICO, "Employment practices and data protection: recruitment and selection", 12 December 2023, (the Guidance) at page 2.
[2] We use the term "candidate" with the same meaning as in the Guidance.

autonomy and control,[3] and of a lack of transparency, explainability, and accountability.

5. Failure to ensure adequate transparency and explainability in the use of AI recruitment techniques means that candidates may not be aware that AI tools are being deployed at all; and if they are, they may not know how they are being used or how to challenge decisions they generate.

6. As with surveillance and algorithmic management of workers once they commence employment, the use of novel technologies and the increased data collection on which they depend can negatively impact worker autonomy and control. This is a point we made in our response to the ICO's consultation on its monitoring at work guidance in January 2023. Although this draft Guidance corresponds to the period before the commencement of an employment relationship, the use of intrusive and opaque recruitment tools raises similar issues. This is particularly in light of the power imbalance between candidates and employers, the scope and extent of the data collected through the use of new technologies in recruitment, and the lack of transparency around how the tools being used function.

7. We understand that the Guidance aims to provide greater regulatory certainty; protect candidates' data protection rights; and help employers and recruiters carry out effective recruitment exercises in compliance with their data protection obligations. We also note the Guidance's rationale for intervention as contained in the impact assessment summary, in particular: the negative externalities that could result from increased discrimination and bias through the use of AI in recruitment as well as the potential for new technologies to lead to regulatory uncertainty for both employers and candidates.

8. These submissions will focus on the section of the Guidance pertaining to automated decision-making (ADM) and profiling for recruitment and selection. We provide suggestions on how the Guidance could provide greater clarity and detail regarding:

    - The implications of involving third-parties in AI recruitment for the data rights of candidates (question 2 of the ICO's survey).
    - The different technologies used, and different types of data collected (question 2 of the ICO's survey).
    - The use of candidate data for training purposes (question 2 of the ICO's survey).
    - The role of Data Protection Impact Assessments (DPIAs) (question 2 of the ICO's survey).

[3] Grimshaw, D. (2020). *International organisations and the future of work: How new technologies and inequality shaped the narratives in 2019*. *Journal of Industrial Relations*, *62*(3), 477-507. https://doi.org/10.1177/0022185620913129.

- Meaningful human intervention and transparency in the context of ADM tools used in recruitment (question 3 of the ICO's survey).

9. For the sake of completeness, we have included the full survey questionnaire in an annex below but have only provided answers in respect of relevant questions.

Survey question 2: How far do you agree or disagree that the draft guidance adequately covers the end-to-end recruitment and selection process and the data protection implications linked to this?

The implications of involving third-parties in AI recruitment for the data rights of candidates

10. The section in the Guidance on the use of third-party AI service providers does not sufficiently cover the nature of the actual roles these services play in recruitment. The Guidance should more closely address which third parties are functioning as (joint) controllers and/or processors.

11. AI recruitment services providers may involve more than one company. For example, an AI service provider's software might rely on another party for its large language model (LLM). In the case of the recruitment chatbot Talenteria, which offers end-to-end recruitment services from CV scoring to AI-conducted interviews to AI recommendations based on "*skills, experience, and education*," each service is powered by ChatGPT.[4] In such instances, candidate data may be processed by both the AI service provider (such as Talenteria) and additional parties integrated in the service (such as Open AI).

12. The Guidance provides that: "*when using AI service providers for recruitment purposes…*" employers "*should consider the types of decisions which may impact their status as a controller for each processing activity.*" We recommend that further detail and examples should be included in respect of the "types of decisions" employers should be considering in order to better achieve the Guidance's aim of regulatory certainty. The Guidance suggests that the decisions could concern: the source and nature of information used to train the AI model, the subject matter of what is trying to be predicted through the AI model, or how the AI model would be continuously tested and updated. These are helpful criteria, but do not provide examples and none of them explicitly cover the decision on the part of an employer to use an AI service provider that in turn relies on a further third-party for its LLM.

13. This is notwithstanding the fact that the potential involvement of multiple actors at different stages of the AI lifecycle with no direct contractual relationship to an employer and/or recruiter could have significant implications for the feasibility of testing and updating the AI algorithm being used. For example, testing for biased outputs is usually more complicated without knowledge of the training dataset

[4] https://www.talenteria.com/landing-ai-recruiting-software.

and its potential biases. Similarly updating and making change to a model one doesn't have control over is not usually feasible, thereby reducing accountability.

14. Whilst Talenteria's website states that its software uses ChatGPT, other similar AI service providers may not make this clear. Without reference to the potential for a service provider to be reliant on an additional third-party, employers and/or recruiters – who the Guidance emphasise have the responsibility as controllers to ensure safe deployment of AI - may not know to look out for such a decision on the part of an AI service provider. We recommend that the Guidance refer to the possibility that other actors, including companies such as Open AI, are identified in the section on "*what else do we need to consider*" (see page 47).

15. The Guidance also does not sufficiently cover the scope of data collection (including the types of data gathered) that takes place through the use of AI algorithms in the recruitment process. The Guidance primarily refers to "data" as a catch-all term, without addressing the different sources from which this data on candidates may be pulled from at all stages of the recruitment process. We further recommend that the Guidance includes detail on the different technologies at play and what categories of data they might gather.

16. The Guidance provides that employers must consider the processing activities that may impact their role as controllers; however, it should reinforce this requirement with specific examples of different data processing activities for different types of AI technologies. We provide a few relevant examples below:

    - CV screening: this would involve the processing of all personal data on the CV in question.
    - AI-conducted interviews: these are likely to take place through Chatbots and may involve data processing via voice detection and facial recognition technology (FRT).[5]
    - Enriched profiles via web-crawling: the algorithm crawls the web to search for publicly available data on the candidate from "*over 20+ social media and public platforms*" to automatically enrich candidate profiles.[6]

17. We consider that information relating to the technology used and the data collected is also relevant to the question of controllership. For example, if an employer uses an integrated end-to-end AI recruitment tool offered by an AI service provider such as Talenteria in respect of all applications, the service provider should be considered as a joint controller. This is because the AI service provider determines what personal data is gathered and the purposes for which it is being collected (i.e., to screen a CV and then conduct an interview via a Chatbot etc.). By contrast, a service provider only supplying a CV screening tool used by an employer in respect of certain applications would be much more likely to only constitute a processor.

[5] See for example: https://www.hirevue.com and https://sapia.ai/ for companies that offer such services.
[6] See https://www.manatal.com/?ssrid=ssr&ssr_id=2x4jlck9bg03yxgs.

18. As above, the Guidance does not make any reference to additional third-parties, such as Open AI, whose tools may be used by the AI service providers' recruitment software. We consider that these additional parties would likely need to be considered data processors given the role that the AI service providers may afford them.[7] We therefore recommend that the Guidance provide further details on when AI service providers and other third-parties may become controllers and/or processors, including through examples that refer to the different technologies used, and types of data collected by their AI technology.

19. The possibility that AI service providers and other actors could be controllers and processors has significant implications for the data rights of candidates. For example, where an AI service provider and a recruiter and/or employer are joint controllers – the full spectrum of data protection rights and obligations would apply to both entities. A lack of clarity in the status of the various parties involved in the recruitment procedure is likely to make it more difficult for candidates to enforce their data protection rights.

Using candidate data for training purposes

20. While the Guidance alludes to machine learning (ML) and the role of training data (see page 45), it does not sufficiently cover this issue as it relates to the role of third parties.

21. The Guidance does not clarify whether (and in what circumstances) AI service providers (and other third parties in the event that a separate entity's LLM is used) can use candidates' personal data (e.g., voice patterns or eye movement data gathered in AI video interviews) to train and retrain their algorithms, which they consequently put back on the market to sell to other employers and/or recruiters. An essential feature of the AI lifecycle is its constant learning and training, which is supported by continuously collected data. This is particularly critical in view of the previously raised role of third-parties as training of the models, as opposed to fine-tuning, will result in data transfers to the third parties providing the technology.

22. We thus consider that the use of large amounts of often highly sensitive, personal data gathered on real-life candidates for training purposes would be difficult to reconcile with a number of data protection rights, namely the right to information, the right to consent, and the right to erasure. The sensitivity of the data being collected (including special categories data, in the form of biometric information, for example) means that it is all the more important that these rights can be effectively relied on in practice.

[7] We note that this logic would apply to other technologies that that a service provider sub-contracts. For example, a company may sub-contract certain parts of their websites (such as a marketplace) to a third party which would then be a data processor. But given the role of AI service providers in the recruitment procedure, we have focused on them here.

23. Firstly, we consider that at the minimum there should be an opt-in mechanism for candidates whose data might be retained by AI service providers to continue to train their model. This should similarly be in place in relation to the sharing of candidates' data by AI service providers with other parties whose tools they integrate into their LLM. Such a mechanism would be in line with the Global Privacy Assembly Resolution on Artificial Intelligence and Employment (the Global Privacy Assembly Resolution), sponsored by the ICO among other organisations, which highlighted how the use of AI in recruitment can result in candidates' "*loss of control over the collection and processing of their personal data*".[8]

24. In view of the power imbalance between candidates and employers, candidates may have little choice but to consent to their data being processed by the AI software in order to go through an interview or recruitment process and consequently may not be aware of where their data ends up along the pipeline. Data processing should consequently only happen for necessary purposes defined by the role of the tool and any additional data collection and processing, for example for training or analytics, should be opt-in and subject to candidates' consent.

25. Secondly, it is not clear from the Guidance how the right of erasure, as protected by Article 17 of the UK GDPR, should apply where an employer or recruiter contracts with an AI service provider that uses candidates' data to train its algorithm. Current research around LLMs and data deletion suggests that deletion is not feasible for the current state of the technology, as deleting a specific data point means, for most standard models, that the whole LLM would need to be re-trained from scratch.[9]

26. There are a number of foreseeable scenarios where this issue could come into play. For example, how would an employer or recruiter comply with an erasure request made by a candidate who initially consented to the use of their data for training purposes, but subsequently withdrew consent and requested deletion under Article 17(1)(b) (absenting the existence of another lawful basis)? In such a scenario, where would the AI software provider come in when the Guidance has largely only considered employers and/or recruiters using the AI software as the responsible controllers?

27. We therefore recommend that the Guidance sets out the need for a clear, contractual relationship between employer and AI service provider that: 1) ensures candidate data is not shared beyond where the candidate expects it to be shared (i.e., to the developers for retraining a model they can sell to other

[8] 45th Closed Session of the Global Privacy Assembly, *Global Privacy Assembly Resolution on Artificial Intelligence and Employment*, October 2023, page 3, https://globalprivacyassembly.org/wp-content/uploads/2023/10/1.-Resolution-on-AI-and-employment-1.pdf.

[9] Ginart, Antonio A., Melody Y. Guan, Gregory Valiant and James Y. Zou. *"Making AI Forget You: Data Deletion in Machine Learning." ArXiv abs/1907.05012 (2019),* https://proceedings.neurips.cc/paper_files/paper/2019/file/cb79f8fa58b91d3af6c9c991f63962d3-Paper.pdf.

employers) and beyond what is necessary for the product to function; and 2) ensures that the employer and other parties process the data in a way that allows candidates to exercise their information rights without detriment (e.g., if a candidate requests a right to delete their data).

The role of DPIAs

28. We welcome the reference to (DPIAs) in the Guidance and in particular the mention of a mandatory requirement to conduct one "*if you plan to use solely or partly automated decision-making and profiling for recruitment purposes*".

29. While the Guidance sets out a promising foundation of what to include in a DPIA in the recruitment context, we recommend that it also includes more specific requirements that employers should be able to evidence, including:

    - What happens with candidate data when using an AI algorithm;
    - How long the data will be retained in the AI service provider's system; and
    - The degree of access and control any third parties have over the algorithm and candidate data.

30. For example, OpenAI states in its data retention policy that it does not utilise business' data to train its models.[10] This is information that employers and/or recruiters could easily obtain and should be required to document in any DPIA they undertake so as to assess how the risks arising from the processing activities could be satisfactorily mitigated.

31. We also recommend that the Guidance clarify that all the sources of data about a candidate processed by the AI recruitment software should be documented in any DPIA(s). This is in line with a set of principles for trustworthy AI in recruiting developed by the US Center of Industry Self-Regulation (CISR), which has produced a number of specific recommendations designed to address this very concern of candidates retaining control over their data.[11] One such recommendation that the Guidance might consider drawing inspiration from is requiring employers to specify in their privacy policy "*the sources of data elements subject to AI processing, if not collected from the candidate themselves*".[12]

32. As we have stated above, the Guidance would do well to clarify in further detail the various forms of ADM and algorithmic tools used in the end-to-end recruitment procedure. This is because the different forms of data collected, and the invasiveness of the technologies used, vary significantly. The varying risks

[10] https://openai.com/enterprise-privacy.
[11] See Center of Industry Self-Regulation (CISR), *Principles for Trustworthy AI in Recruiting and Hiring*, https://assets.bbbprograms.org/docs/librariesprovider5/default-document-library/cisr_ai-hiring-principles_2023.pdf?sfvrsn=29b3a3fc_6&_ga=2.175393322.986918920.1694524939-1906595052.1691757788.
[12] *Principles for Trustworthy AI in Recruiting and Hiring.*

stemming from the technologies used in this context was acknowledged in the Global Privacy Assembly Resolution, which stated that:

> *"…and more generally any form of 'biometric categorisation', is high risk and should in most cases be prohibited in the employment context, and if used in limited and defined cases must be subject to appropriate safeguards including robust testing and/or other assessments to ensure that such systems use valid and reliable methodologies and operate as intended*".[13]

33. We recommend that the Guidance specify different categories or levels of AI recruitment software so employers can better tailor their DPIAs according to the risk level of different technologies. We further recommend that the Guidance makes clear that where employers and/or recruiters are using multiple systems for different purposes (including where a single AI provider offers an integrated system across the recruitment procedure), they will need to conduct discrete assessments of the risks to data subjects for each one used. This could be undertaken by way of a single DPIA or multiple ones each relating to the system or technology being used.

34. The above recommendations would ensure that the minimum requirements of a DPIA are more effectively adhered to, namely that: the assessments cover the nature, scope, context, and purposes of the processing; its necessity and proportionality; the risks presented to data subjects; and any mitigating steps.

Question 3: How far do you agree or disagree that the draft guidance contains the right level of detail?

Meaningful human intervention and transparency in the context of ADM tools used in recruitment

35. We welcome the detail the Guidance provides on what constitutes meaningful human involvement to ensure that a particular ADM tool does not constitute solely automated processing. However, the Guidance should provide further detail on what actually constitutes a "decision" for the purposes of ADM in the recruitment context.

36. We note that the Guidance refers to "recruitment decisions" as those that have legal or similarly significant effects on candidates. It gives a few examples, including: "*a decision about whether to shortlist a candidate, recommend them for interview, reject them or promote them*" (see page 37).

37. We consider that the Guidance should go further in this regard. In the case of tools offered by companies such as Talenteria, AI algorithms are regularly providing scores or recommendations that correspond to the recruitment

[13] Global Privacy Assembly Resolution, page 3.

decisions outlined above (such as whether to hire a particular candidate). It is submitted that the Guidance already implicitly acknowledges that these can themselves constitute decisions. For example, it recognises that "solely automated outputs" will constitute decisions within the remit of Article 22(1) of the UK GDPR if there is no meaningful involvement at each stage of the recruitment process. The Guidance states that meaningful review would require humans to have sufficient power to overturn AI recommendations or predictions; not to attach disproportionate weight to the AI outputs; and to have training in relation to ADM (among other criteria).

38. By the same logic, AI outputs where these requirements are not met would constitute solely ADM as prohibited by Article 22(1) of the UK GDPR. For example, if an AI recommendation regarding the candidates to shortlist was always followed this would naturally constitute solely automated ADM and would be unlawful unless the employer could rely on one of the exceptions at Article 22(3) of the UK GDPR.

39. We therefore recommend that the Guidance explicitly clarify that AI outputs (such as recommendations or predictions) can themselves constitute a decision with legal or similarly significant effects on candidates if (a) the output is in effect "rubber-stamped"; and (b) if the outputs correspond to one or more of the recruitment decisions in the Guidance and listed above. It is noted that the European Court of Justice took the same approach in its judgement in the recent *SCHUFA* case in which it found that a credit reference agency engaged in solely ADM when generating credit repayment probability scores where lenders drew heavily on these scores in decisions as to whether to grant an individual credit.[14]

40. This is analogous to employers drawing heavily on the recommendations and/or predictions of a third-party AI algorithm in decisions such as whether or not to shortlist a candidate to interview. In *SCHUFA*, it was the third-party that carried out solely ADM contrary to Article 22(1) of the GDPR. However, this was because there was no joint controllership between the lenders and the credit repayment agencies given that the decisions on the purpose and means of processing were wholly distinct. As we have seen above (and as recognised by the Guidance), there may be scenarios where an employer and a third-party AI service provider act as joint controllers. Therefore, it is in the interests of regulatory certainty for the Guidance to clarify that the outputs may themselves constitute decisions with legal or other significant effects.

41. Such an approach would result in enhanced accountability on the part of employers and/or recruiters. This is because it would encourage more vigorous testing, documented in DPIAs and audits or other tests, regarding the extent to which human review is in fact being implemented. As such, we recommend that the Guidance provide additional detail on the need for statistical testing to

[14] Case C-634/21 *SCHUFA* [2023] ECLI:EU:C:2023:957

monitor the percentage of cases where a reviewer does not follow the AI output and vice versa.

42. Finally, we consider that the Guidance should provide additional detail as to how employers and/or recruiters can affect transparency when relying on ADM in the recruitment process. This would further the aim, as set out in the Global Privacy Assembly Resolution, of ensuring that employees and unions are able to understand AI systems' "purpose, how they work, and the metrics used," in a comprehensible way.[15]

43. Firstly, the Guidance's section on the need to provide meaningful details regarding the logic involved in ADM systems does not refer to the role of third-parties. As we have shown, it will often be AI service providers who develop the systems used by an employer or recruiter. We therefore recommend that the list of points that should be explained to candidates (see page 43) refers to the role of third-parties so that the information provided encompasses their uses of data. This avoids the situation of companies failing to meet transparency and explainability requirements by relying on third-parties.

44. Secondly, we consider that the list of explanatory information to be provided could be further augmented. For example, the Article 29 Data Protection Working Party's *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679* (the Guidelines) state that the meaningful information should include the categories of data used in the decision-making process.[16]

45. The current framing in the Guidance states that the meaningful details should include the information candidates will be asked to provide. This is overly broad and ignores the fact that certain categories of data may be processed without the candidate being asked to provide them. This could include image data taken during a Chatbot interview and inferred data derived from a candidate's facial expression or voice regarding their performance.

46. Similarly, we recommend following the Guidelines, which refer to the need to explain why particular categories of data are deemed pertinent in the context of ADM. This is particularly significant in relation to inferred data, which may be critical to a recruitment decision but that as above is not covered by the ICO's Guidance.

47. We further recommend the inclusion of information relating to statistical analysis (both its use and forms) both with respect to the generation of a particular AI output (for example a prediction, profile, or recommendation) and when testing for fairness and accuracy.

---

[15] Global Privacy Assembly Resolution, page 2.
[16] Article 29 Data Protection Working Party, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, https://ec.europa.eu/newsroom/article29/items/612053/en, page 31.

48. Finally, we note that the Guidance states that the provision of source code is unlikely to result in the disclosure of commercially sensitive information. On this basis, we recommend that the Guidance state that it would be best practice for an employer and/or recruiter to provide transparency and explainability materials related to the technology deployed, including the means, necessary data, and role of those systems. The Guidance could suggest that where possible they provide an API to allow the code to be tested with synthetic data in order to enable the audit of the algorithms used by worker representatives, public authorities and/or independent third parties.

49. We recommend that the Guidance provide that in the alternative employers and/or recruiters provide the name and description of any models used, potentially including easy-to-understand diagrams or images.

Conclusion

50. Recruitment is a complex and multi-layered process, and so is the AI technology intended to service this process at one or all stages of it. Whilst the Guidance sets up an important foundation for assessing the legal and ethical implications of employers and/or recruiters deploying AI in their recruitment and selection processes, it lacks the detail needed to address the complexities of the technology's various affordances.

51. The Guidance overlooks notable complexities in the AI lifecycle that must be addressed in more detail both in a revision of this Guidance and in more specific recommendations for conducting DPIAs. The Guidance would do well to incorporate our above recommendations on addressing the various roles of third-party AI service providers – particularly as pertains to multiple actors – and their controller/processor status; clarifying the data-sharing relationship between candidate and employer with regards to the AI recruitment service; and providing more detail on adjudicating ADM in AI recruitment decisions. The technical and legal submissions serve to ensure that the deployment of AI in the recruitment cycle does not harm candidates or compromise their data protection and information rights.

Appendix 1

Q1 How far do you agree or disagree that the draft guidance is clear and easy to understand?

☐ 1 – Strongly agree
☐ 2 – Agree
☐ 3 – Disagree
☐ 4 – Strongly disagree
☐ 5 – Unsure/don't know

Please give reasons for your choice:

Q2 How far do you agree or disagree that the draft guidance adequately covers the end to end recruitment and selection process and the data protection implications linked to this?

☐ 1 – Strongly agree
☐ 2 – Agree
☒ 3 – Disagree
☐ 4 – Strongly disagree
☐ 5 – Unsure/don't know

Please explain your choice. If you disagree, strongly disagree, or are unsure, please outline what additional areas you would like to see covered:

See body of our response above.

Q3 How far do you agree or disagree that the draft guidance contains the right level of detail?

☐ 1 – Strongly agree
☐ 2 – Agree
☒ 3 – Disagree
☐ 4 – Strongly disagree
☐ 5 – Unsure/don't know

Please explain your choice. What, if any, changes or improvements would you like to see?

See body of our response above.

Q4 How easy or difficult is it to find information in the draft guidance?

☐ 1 – Very easy
☐ 2 – Easy
☐ 3 – Difficult
☐ 4 – Very difficult
☐ 5 – Unsure/don't know

Please explain your choice. What, if any, changes or improvements would you like to see?

Q5 Please provide details of any cases, examples, scenarios or online resources involving recruitment and selection that would be useful for us to include in the guidance.

Q6 Please provide any other suggestions for the draft recruitment and selection guidance:

Q7 Do you use social media for recruitment and selection purposes?

☐ 1 – Yes
☐ 2 – No
☐ 3 – Unsure / don't know

If yes, please provide further details on the types of social media and how you use them for recruitment and selection:

Q8 Do you use AI or other technologies to process personal information for recruitment and selection purposes?

☐ 1 – Yes
☐ 2 – No
☐ 3 – Unsure / don't know

If yes, please provide further details. In particular, please explain whether you rely on any of the Article 22(2) exceptions in UK GDPR to allow you to carry out the processing.

Q9 How far do you agree that the impact assessment summary adequately covers the main affected groups?

☐ 1 – Strongly agree
☐ 2 – Agree
☐ 3 – Disagree
☐ 4 – Strongly disagree
☐ 5 – Unsure/don't know

If you disagree, strongly disagree or are unsure/don't know, please provide examples of any affected groups you think we have missed or require further consideration:

Q10 How far do you agree that the impact assessment summary adequately outlines the main impacts?

☐ 1 – Strongly agree
☐ 2 – Agree
☐ 3 – Disagree
☐ 4 – Strongly disagree
☐ 5 – Unsure/don't know

If you disagree, strongly disagree or are unsure/don't know, please provide details of any impacts we have missed or that require further consideration:

Q11 Are you responding to this consultation on behalf of an organisation?

☒ 1 – Yes
☐ 2 – No

If no, please skip to Q17.

Q12 Who in your organisation needs to read the guidance? (Please provide job titles or roles and how many people in those roles would be expected to read it, not people's names)

Q13 To what extent (if at all) do data protection issues affect strategic or business decisions within your organisation?

☐ Data protection is a major feature in most of our decision making
☐ Data protection is a major feature but only in specific circumstances
☐ Data protection is a relatively minor feature in decision making
☐ Data protection does not feature in decision making
☐ Unsure/don't know

Q14: Do you think the draft recruitment and selection guidance would result in additional costs or benefits to your organisation? (These could be financial or non-financial and might include staff time)

Please select the most relevant option below:

☐ cost(s) or burden(s)
☐ benefit(s)
☐ both
☐ neither
☐ Unsure/don't know

if you answered neither or unsure/don't know, please skip to Q17

Q15 Could you please describe the types of additional costs or benefits you might incur?

Q16 Can you provide a rough estimate of the costs or benefits you are likely to incur and briefly how you have calculated these?

Q17 If there is any other evidence or information on the potential impact of the guidance or our impact assessment summary that you would like us to consider, please provide it in the box below. This could include a description, links to other sources, or contact details where we can reach you to discuss further.

Q18 How did you find out about this consultation?

☐ ICO website
☐ ICO Twitter account
☐ ICO Facebook account
☐ ICO LinkedIn account
☐ ICO staff member
☐ ICO newsletter
☐ colleague from your organisation
☐ person outside of your organisation
☐ other
If other please specify:

Q19 Who are you responding as?
(please tick all that apply)

☐ an organisation or person employing workers
☐ a recruitment agency
☐ a representative of a professional, industry or trade association
☐ an organisation representing the interests of employees, workers, self-employed (eg charity, employment advocacy organisation)
☐ an employment rights professional body or advice service
☐ a trade union
☐ an academic
☐ a supplier of employment technology solutions (eg monitoring software or HR systems)
☐ an individual acting in a private capacity (eg someone providing their views as a member of the public)
☐ an ICO employee
☐ other
If other please specify:

If you are acting only as an individual acting in a private capacity, please skip to Q22.

Q20 Please provide the name of your organisation:

Privacy International

Q21 What is the size of your organisation?

☐ Micro-organisation (less than 10 members of staff)
☐ Small or medium organisation (10-249 members of staff)
☐ Large organisation (250 members of staff or above)
☐ Not applicable or not sure

Q22 Finally, 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 an email address:
