1. Could restart the security and privacy champions network to help ensure that privacy and data protection is embedded at a local level across all teams that process personal data. This will also help to support and provide resilience to the internal information security team and outsourced legal counsel and information security consultancy.
2. Could consider what other measures may be used to support the same aim of raising awareness and deploy them in combination with the phishing exercises. Whilst the use of regular phishing exercises can be one way for an organisation to raise staff awareness around information security and data protection matters, there is a risk that staff may become complacent or disengaged with the practice if it is too often repeated over a period of time.
3. Could update relevant policies, procedures and staff guidance materials so they refer to specific job titles rather than named individuals. This means that should an individual staff member leave the organisation, the relevant document would not need to be updated and would continue to provide accurate information about, for example, which job roles were involved in its implementation.
4. Could update relevant policies, procedures and staff guidance materials so they refer to specific job titles rather than named individuals. This means that should an individual staff member leave the organisation, the relevant document would not need to be updated and would continue to provide accurate information about, for example, which job roles were involved in its implementation.
5. Could introduce compliance metrics or KPIs for individual rights requests – such as number of requests processed and % compliance with the statutory timeframe – which may help to ensure that compliance is monitored appropriately and improve performance and processes.
6. Could review the HR policy and other policies to ensure that staff with privacy-related questions are directed to the correct email address, rather than an outdated email address.
7. Could consider whether it is necessary to indefinitely retain all candidate personal data for model development and testing, or if the same outcomes might be reached using only a subset of retained data. Although the UK GDPR does not apply to personal data that has been fully and irreversibly anonymised, retaining less data would reduce the resource cost of prolonged data storage, and reduce the risk of reusing data where candidate characteristics have been inferred which may be

inaccurate as in **[REDACTED]**. In an event where the retained data can be re-identified using a key or where a characteristic population is very small, this will also avoid non-compliance with UK GDPR article 5(1)e.

8. Could ensure mechanisms are in place to identify any personal data – including special category or criminal offence data – that is accidentally collected such as in candidate free text application responses and where a lawful basis or additional condition have not been selected, and delete it before the data is processed. This will help to ensure accidentally collected personal data is not processed by AI tools and reduces the impact on individuals in the event of a personal data breach.
9. Could review whether retained personal data will be used to train a new and separate AI model – rather than only to refine existing AI models – as this is likely to be considered a new purpose for processing personal data. This new purpose for processing should be transparent to individuals as in **[REDACTED]**, and if acting as data processor the organisation would need explicit permission for this processing as in **[REDACTED]**.
10. Could consider whether it is necessary to indefinitely retain a subset of candidate personal data for model development and testing, or if the same outcomes might be reached using less data still. Although the UK GDPR does not apply to personal data that has been fully and irreversibly anonymised (aggregated in this case), retaining less data would reduce the resource cost of prolonged data storage. In an unlikely event where the retained data can be re-identified using a key or where a characteristic population is very small, this will also help to avoid non-compliance with UK GDPR article 5(1)(e).
11. Could periodically test the personal data breach process, by holding walkthrough exercises or desktop scenarios/ simulations with key staff. This could help to ensure that personal data breach management processes remain effective and reduce the risk of detrimental impact to an individual's privacy and rights.
12. Could undertake more regular reviews of user access rights than the current quarterly and half yearly reviews that take place. This will help to provide further assurance that all staff only have access to the systems and apps at the appropriate level that they need to perform their role, and will help to more quickly identify and revoke any user access permissions that may be missed during the movers and leavers process.

13. Could undertake more regular reviews of user access rights than the current half yearly reviews that take place. This will help to provide further assurance that all staff only have access to the systems and apps at the appropriate level that they need to perform their role, and will help to more quickly identify and revoke any user access permissions that may be missed during the movers and leavers process.
14. Could consider rotating the firm it uses as an external security audit provider every set number of years. This rotation will help to ensure each provider has an independent and unbiased approach to the external audit process and will reduce any potential conflicts of interest arising from long-standing auditor-client relationships.
15. Could undertake periodic user testing of its privacy information to help provide assurance that it is sufficiently understood by the intended audience. Feedback from individuals could be used to inform potential improvements in the design, content, channels and points in the user journey where privacy information is presented. The ICO's website contains guidance on user testing of privacy information.
16. Could undertake periodic user testing of its privacy information to help provide assurance that it is sufficiently understood by the intended audience. Feedback from individuals could be used to inform potential improvements in the design, content, channels and points in the user journey where privacy information is presented. The ICO's website contains guidance on user testing of privacy information.
17. Could undertake periodic user testing of its privacy information to help provide assurance that it is sufficiently understood by the intended audience. Feedback from individuals could be used to inform potential improvements in the design, content, channels and points in the user journey where privacy information is presented. The ICO's website contains guidance on user testing of privacy information.
18. Could review analytics data to assess what proportion of candidates actually access the relevant privacy notice before their personal data is collected during the assessment, and determine whether there are any design changes that could be made which would lead to more candidates accessing this privacy information.
19. Could review analytics data to assess what proportion of candidates actually access privacy information before their personal data is collected, and determine whether there are any design changes that

could be made which would lead to more candidates accessing this information.

20. Could provide a link in the **[REDACTED]** to the **[REDACTED]** privacy notice in addition to the **[REDACTED]** privacy notice. This will help to ensure that candidates have a further way of accessing relevant privacy information regardless of the platform they use to undertake their assessment.
21. Could provide a suitably prominent link to its **[REDACTED]** in any relevant privacy information it provides to candidates, to help ensure that individuals are adequately informed about how **[REDACTED]** works and how the assessment results are used by the organisation and its clients.
22. Could provide the name and contact details of the supervisory authority that individuals are most likely to complain to if they have a problem in privacy information. For UK data subjects this is likely to be the Information Commissioner's Office (ICO). The ICO's contact details are:
    - Website: https://ico.org.uk/
    - Telephone: 0303 123 1113
23. Could conduct user testing with individuals to evaluate how well understood its privacy information is. Based on any feedback received, the organisation could implement improvements to the content, style and presentation of privacy information so individuals are better informed about use of their personal data.
24. Could produce privacy policies that are targeted to specific individuals/ use cases and tailored to the requirements of specific legislation eg the UK GDPR. This may help to ensure that individuals are provided with sufficient specific detail about how their data is processed, without combining separate use cases in one large document that might be confusing, misleading, or inaccessible.
25. Could improve the DPIA by including a data flow diagram to show the relationships and data flows between the tool and other stakeholders involved in the relevant processing activities.
26. Could record the review frequency or date of next review in the relevant DPIA document, to help ensure that DPIAs are subject to periodic scheduled review.
27. Could include each individual's job title alongside their name or email address, to make it clearer about which staff have been involved in the completion and approval of DPIAs.

28. Could signpost more relevant ICO guidance in DPIA template documents, such as pages available in ICO DPIA guidance.
29. Could take steps to ensure that the correct name for sign-off of DPIAs is included, to embed recent changes in structure and responsibilities in relation to data protection management.
30. Could update its **[REDACTED]** to ensure the differences between EU GDPR and UK GDPR are noted.
31. Could ensure that its template DPIA includes sufficient information to assure clients of data protection measures in place and assist them in complying with UK GDPR article 35, including but not limited to:
    - the proposed personal data processing and consideration of alternative approaches,
    - a clear explanation of the relationships and data flows (based on a data flow mapping) between controllers, processors, individuals and systems,
    - how data processing will comply with the statutory data protection principles,
    - a comprehensive assessment of the privacy risks to the rights and freedoms of individuals,
    - mitigating controls implemented by the organisation to reduce these privacy risks.

    The ICO has produced guidance on completing DPIAs for AI.
32. Could support its clients in reviewing their DPIAs, by undertaking a regular meaningful review of its own template DPIA, particularly when there is a system change or change to data processing, when new or changes to privacy risks are identified, and when there are product performance or KPI issues. This will help to ensure that data processing and the risks involved are detailed accurately and support compliance with UK GDPR article 35(11).
33. Could work with appropriate external partners to subject its AI algorithmic codes to independent reviews or audits.
34. Could provide its clients with documentation that outlines the measures it takes to minimise bias and discriminatory outputs in its AI models and systems. This will help **[REDACTED]** and its clients demonstrate that its products produce fair outcomes and will help to meet UK GDPR article 5(1)(a) requirements.
35. Could have a complaints log in place in order to record complaints or negative feedback to look for trends which may need to be addressed.

36. Could regularly review risks of accuracy and bias and consider how it can prove the unbiased nature and statistical accuracy of its models. This will help them to achieve **[REDACTED]**.
37. Could start to monitor algorithmic KPIs and use these as a part of a documented decision making process when developing and testing models.
38. Could consider algorithmic fairness limitations and how they can be navigated, such as where protected characteristics are unequally distributed or where an individual fits multiple protected characteristics. This will help to reduce the risk of processing personal data in a way that is unfair or has an unfair outcome on specific groups of individuals, and support compliance with UK GDPR article 5(1)(a). The ICO has further guidance on considerations around algorithmic fairness.
39. Could consider algorithmic fairness limitations and how they can be navigated, such as where protected characteristics are unequally distributed or where an individual fits multiple protected characteristics. This will help to reduce the risk of processing personal data in a way that is unfair or has an unfair outcome on specific groups of individuals, and support compliance with UK GDPR article 5(1)a.
40. Could formalise periodic quality checks on human changes to assessment algorithms or outputs, to reduce the risk of errors or bias unintentionally being introduced.
41. Could assess the risk of their AI tool being used alone to make recruitment decisions by clients, which would subject candidates to decisions based solely on automated processing and which produce legal or similarly significant effects on them. While this is the responsibility of the data controller, documenting the risk and appropriate risk treatment measures or controls – such as documenting the need for human reviews in contracts and providing example training materials – will help to evidence compliance with UK GDPR article 22.
42. Could assess the risk of **[REDACTED]** being used alone to make recruitment decisions by clients, which would subject candidates to decisions based solely on automated processing and which may be considered to produce legal or similarly significant effects on them. While this is the responsibility of the data controller, documenting the risk and appropriate risk treatment measures or controls already in place – such as documenting the need for human reviews in contracts and client literature – will help to evidence compliance with UK GDPR article 22.