Browne Jacobson

Using AI for recruitment: The data issues

13 June 2025 Richard Nicholas and Saara Leino

Like toddlers' fingers and electric sockets, the advice when it comes to personal data and AI, is usually to keep the two as far apart as possible – keep the personal data away from the AI.

But what about areas such as HR and recruitment, where there can be no easy separation of personal data, because all of the data being managed concerns people?

I've touched on this before in this article – the eight questions (A-i) to ask before introducing personal data to AI, which is worth a read - however in this article we'll be looking at a recruitment audit report kindly carried out by the ICO and will be drawing from the conclusions of that report.

Key findings

The findings of the audit are important for HR teams but also for the providers of AI tools to those teams, since every requirement on a recruiter is likely to be a feature request for tools being developed, or might even make the difference between a tool being chosen or ignored.

We've set out below the seven key recommendations and what that means for HR teams and the providers of AI tools to them.

The seven key recommendations

Helpfully, ICO also lists seven recommendations to ensure compliance with the data protection legislation and good practice. The key recommendations are:

1. **Fairness:** HR teams and users of AI tools must continuously monitor AI systems for bias and inaccuracy and take appropriate steps to address them. Especially when special category personal data is processed. AI providers should be able to help address issues as they arise.
2. **Transparency and explainability:** Recruiters must inform candidates about the AI processes that their data will undergo, ensuring that privacy information is clear and comprehensive. Developers must help recruiters to provide this information.
3. **Data minimisation and purpose limitation:** AI systems should only collect essential data required for the purpose to be carried out and strictly adhere to the intended purposes of data processing. The ICO has indicated on several occasions that to training, testing or developing AI tools using personal data that has already been collected, may well breach this obligation. If you don't have a legal basis that is consistent with the original collection then use synthetic data instead.
4. **Data Protection Impact Assessments (DPIAs):** To ensure the safety of the candidates, a risk assessment called DPIA is required when new technologies are introduced. This should be conducted early in the AI development phase and updated as necessary to address any potential risks to data subjects.
5. **Data controller and processor roles:** Defining the data protection roles of recruiter and AI developer is essential to ensure that both parties are processing data lawfully. Depending on the technical implementation and whether the tool is a tailored or off-the-shelf solution, the roles of the parties may change during the processing. The AI developer is usually the controller in respect of personal data used to train the system but the Recruiter will be the controller for input data once the system is live. It is worth spending sufficient time to ensure that the sources of data in different phases align with the correct roles of the parties.
6. **Explicit processing instructions:** The ICO also emphasised the importance of third-party relationships and the importance of having

a data processing agreement in place with enough detail to cover each specific processing operation.

7. **Lawful basis and additional conditions:** Finally, the ICO reminds that everyone needs to have a lawful basis for processing personal data for AI related purposes, especially when handling special category data. Be careful when using consent or legitimate interest, especially if the AI system is used to make automated decisions and remember that the information you provide for the candidates needs to reflect the chosen legal basis in order for it to be valid.

What does this mean in practice?

If you are in the process of deploying AI-powered tools as part of your recruitment process, and particularly if you develop those tools, it would be worth familiarising yourself with the report.

Below you will find some of the recommendations inspired by the report we'd suggest for organisations either developing or using artificial intelligence tools for recruitment.

Use Case	Recommendations for AI Providers	Recommendations for Recruiters
Candidate Sourcing	Ensure that AI tools collect only the necessary personal data and avoid scraping excessive information from online profiles. Ensure that your customers know the different data protection roles at each step of the process.	Verify that the AI tools used respect candidates' privacy and comply with data protection laws. Ask for the origin of the data used to train the system. Communicate transparently with candidates about how their data is sourced and used. Clearly define the lawful basis for processing data and inform candidates about its use.
Application Screening	Design algorithms that prioritise fairness and accuracy, avoiding biases that could lead to discrimination. Regularly test and audit the tools to ensure compliance with ethical standards. Ensure that screening data is not stored in log files or other places where they can be accessed by unauthorised persons.	Regularly monitor AI-generated rankings to ensure they align with organisational values and do not unfairly exclude candidates. Use AI as a support tool rather than a sole decision-maker. Ensure that organisation has role-based access management protocols in place, enabling only authorised and trained personnel to access the data. For automated decision making have a process in place to ensure that a human can, where requested, independently review those decisions.
Bias Detection	Incorporate mechanisms to monitor and mitigate biases in AI systems and update the mechanisms regularly to align with industry best practices. Avoid inferring sensitive characteristics like gender or ethnicity without explicit	Look at ways in which AI tools to promote diversity and inclusion (for instance removing barriers that might exclude certain candidates) but validate their outputs with human oversight.

	consent but use special category personal data to the extent it is necessary to ensure the fairness of the system.	Ensure that hiring decisions are not solely based on AI-generated data.
Efficiency Gains	Develop intuitive systems that automate repetitive tasks while maintaining high standards of data security and integrity.	Leverage AI to streamline administrative tasks, allowing recruiters to focus on strategic decision-making. Ensure that efficiency does not come at the cost of fairness or transparency.
Decision Support	Provide clear and interpretable outputs that allow recruiters to understand the rationale behind AI-generated decisions Help recruiters to understand the logic of the algorithms and previous test data to the extent it is needed for transparency purposes.	Combine AI insights with human judgment to make balanced and informed hiring decisions. Maintain accountability for final decisions, ensuring they align with ethical practices. If you were asked to explain the AI assisted decision before a court you will want to be able to demonstrate that you had controls in place to ensure that decisions made were fair. To do that you will need a practice of monitoring the decisions made and the right governance structure in place.

Contact

Richard Nicholas

Partner

richard.nicholas@brownejacobson.com

+44 (0)121 237 3992

Saara Leino

Professional Development Lawyer

saara.leino@brownejacobson.com

+44 (0)330 045 1289

Related expertise

AI regulation and governance

Data protection and privacy

Employment

HR services