BCLP. Client Intelligent

Insights

AI TOOLS IN RECRUITMENT – KEY TAKEAWAYS FROM THE ICO REPORT

Dec 04, 2024

SUMMARY

On 6 November 2024, the ICO published an outcomes report on AI tools in recruitment (the "Report"). This Report follows consensual audit engagements carried out by the ICO with developers and providers of AI tools to be used in recruitment between August 2023 and May 2024 and is part of the ICO's ongoing upstream monitoring of the wider AI ecosystem to ensure compliance with UK data protection law.

These audits revealed that some AI tools were not processing personal data fairly, for example by inferring characteristics such as gender and ethnicity from an individual's name or by allowing recruiters to filter out applicants with protected characteristics. The ICO auditors also found that some AI tools seemed to be collecting far more personal data than necessary to achieve its purpose and that this data was being retained indefinitely without the candidate's knowledge. They subsequently made 296 recommendations to the developers and providers of AI tools that were audited which covered a range of areas with the aim of improving and ensuring data protection compliance and management of privacy risks.

We set out below some of the key takeaways of the Report.

FAIRNESS

The ICO notes in the Report that recruiters and AI providers must make sure they are processing personal information fairly in their use of AI. The ICO clarifies that this obligation includes monitoring the AI system for any potential or actual accuracy or bias issues and taking steps to address these and that those using AI should ensure that any data processed to monitor for discriminatory issues is adequate and accurate enough to be effective and should also ensure this processing complies with the relevant data protection laws.

TRANSPARENCY AND EXPLAINABILITY

The ICO reminds recruitment teams that they must ensure that they provide detailed information on how they will be processing candidates' personal data. The Report suggests that this information should clearly explain (i) what personal information is being produced by the AI tools (and how); (ii) how the business is using personal information in its development of the AI system; and (iii) the methodology involved in producing any outputs.

The ICO recommends that AI providers should support this obligation by providing the recruiter with the relevant technical information.

DATA MINIMISATION AND PURPOSE LIMITATION

For AI providers, the Report suggests that they should comprehensively assess the minimum amount of personal information required to develop and operate the AI, how long they should be holding the data for and the purpose behind processing this specific data.

The ICO further recommends that recruiters should take a targeted approach and only collect the minimum personal information necessary to achieve the intended purpose of the AI and that they should confirm that the personal information is only being processed for that specific purpose and that it is not being stored or reprocessed for any alternative purpose. The guidance also suggests that the period for retention of such data should be recorded in privacy information, contracts and a retention schedule.

DATA PROTECTION IMPACT ASSESSMENTS (DPIA)

The Report suggests that AI providers and recruiters should complete a DPIA early in the development of the AI tool and prior to processing the personal information, particularly where processing is likely to result in a high risk to individuals and that the DPIA should be updated as the AI develops and as and when the processing changes.

The Report provides detail on what must be included in the DPIA such as (i) a comprehensive assessment of privacy risks to people whose personal information is being processed; (ii) appropriate controls to mitigate and reduce these risks; and (iii) an analysis of the balance between people's privacy and other competing interests.

DATA CONTROLLER AND PROCESSOR ROLES

The ICO further recommends that AI providers and recruiters must define whether the AI provider is the controller, joint controller or a processor for each instance of processing of personal information and ensure this is recorded clearly in privacy information and contracts.

EXPLICIT PROCESSING INSTRUCTIONS

The ICO also expresses that those involved in the hiring process must set clear and detailed processing instructions for their AI provider to follow when they are processing personal information on the organisation's behalf. The guidance suggests that the recruitment team should check that their AI providers are complying with these instructions and that the AI providers should make sure to follow these specific instructions when processing personal data on behalf of the recruiter.

LAWFUL BASIS AND ADDITIONAL CONDITION

Finally, the ICO provides that AI providers and recruiters must: (i) identify the lawful basis they relied on for each instance of personal data processing where they are the controller, before processing any information; (ii) identify an additional condition in circumstances where they are processing special category data; document the lawful basis and condition in privacy information and contracts; (iii) complete a legitimate interests assessment where necessary; and (iv) when relying on consent, ensure the consent is appropriately logged and is as easy to withdraw as it was to give.

Undoubtedly, the use of AI tools in the employment context has strong potential to bring benefits such as saving time and money in the recruitment process, but at the same time it can also create significant risks if the tools are not deployed lawfully and carefully by organisations. AI in the context of employment and worker's management is one of the areas that is identified under the EU AI Act as being high-risk and the AI Act puts strict obligations on deployers of such tools. As detailed above, the ICO has now set out ground rules and best practices for organisations to rollout AI tools in recruitment to ensure data protection compliance and to best manage privacy risks.

Organisations planning to use AI tools in HR should therefore familiarise themselves with the recommendations set out by the ICO in the Report and consider if any requirements under the EU AI Act apply to them, taking a careful approach when rolling out any AI tools.

RELATED PRACTICE AREAS

- Data Privacy & Security
- Employment & Labor

MEET THE TEAM

Geraldine Scali

London

geraldine.scali@bclplaw.com
+44 (0) 20 3400 4483

Olivia Wint

London

olivia.wint@bclplaw.com
+44 (0) 20 3400 4621
